TERMO DE REFERÊNCIA

Processo nº 00196.004611/2024-62

Área: Departamento de Tecnologia da Informação e Comunicação

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação, por meio do Sistema de Registro de Preços (SRP), de Solução Integrada de Serviços de Segurança e de Serviços de Conectividade de Rede, compreendendo: provimento de serviços de segurança de rede e endpoints; monitoramento e administração dos serviços providos; resposta a incidentes de segurança; fornecimento de solução de conectividade para rede local e wireless; instalações e configurações das soluções providas e treinamento para a equipe do Cofen, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE 1									
Item	**Descrição do Serviço**	**CATSER**	**Desembolso**	**Métrica ou Unidade de Medida**	**Quant. (a)**	**Valor Unitário/Mensal (b)**	**Valor Mensal (c) = (a) x (b)**	**Valor Anual (12 meses)**	**Valor Total (60 meses)**
1	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	27014	mensal	unidade	2	R$ 46.100,56	R$ 92.201,12	R$ 1.106.413,44	R$ 5.532.067,20
2	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	27014	mensal	unidade	2	R$ 37.998,18	R$ 75.996,36	R$ 911.956,32	R$ 4.559.781,60
3	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	27014	mensal	unidade	2	R$3.497,33	R$ 6.994,66	R$ 83.935,92	R$ 419.679,60
	Instalação da solução de proteção do								

4	tráfego de rede de próxima geração (on premise) do Tipo A	27111	único	unidade	2	R$ 17.000,00	R$ 34.000,0	R$ 34.000,00	R$ 34.000,00
5	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	27111	único	unidade	2	R$ 17.000,00	R$ 34.000,0	R$ 34.000,00	R$ 34.000,00
6	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	27111	único	unidade	2	R$ 17.000,00	R$ 34.000,0	R$ 34.000,00	R$ 34.000,00
7	Serviços Técnicos Especializados	27332	sob demanda	horas	50	R$ 191,00	R$ 9.550,00	R$ 114.600,00	R$573.000,00
8	Treinamento da Solução de Serviços Gerenciados de Firewall	16837	único	unidade	1	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00
9	Serviços de Solução de proteção para Estações	27502	mensal	unidade	500	R$ 16,50	R$ 8.250,00	R$ 99.000,00	R$ 495.000,00
10	Serviços de Solução de proteção para Servidores	27502	mensal	unidade	200	R$ 16,50	R$ 3.300,00	R$ 39.600,00	R$ 198.000,00
11	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações	27014	mensal	unidade	500	R$ 16,50	R$ 8.250,00	R$ 99.000,00	R$ 495.000,00
	Serviços de detecção e								

12	resposta 24/7, suportado pelo fabricante da solução de proteção para servidores	27014	mensal	unidade	200	R$ 16,50	R$ 3.300,00	R$ 39.600,00	R$ 198.000,00
13	Instalação da solução de Segurança de Endpoints, Detecção e Respostas	27260	único	unidade	500	R$ 122,17	R$ 61.085,00	R$ 61.085,00	R$ 61.085,00
14	Instalação da solução de Segurança de Servidores	27260	único	unidade	200	R$ 122,17	R$ 24.434,00	R$ 24.434,00	R$ 24.434,00
15	Treinamento da Solução de Endpoints	3840	único	unidade	1	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00
16	Serviços de Conectividade Wireless	27014	mensal	unidade	80	R$ 51,00	R$ 4.080,00	R$ 48.960,00	R$ 244.800,00
17	Instalação da solução de Conectividade Wireless	27111	único	unidade	80	R$ 240,00	R$ 19.200,00	R$ 19.200,00	R$ 19.200,00
18	Treinamento da Solução e Conectividade Wireless	16837	único	unidade	1	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00	R$ 8.000,00
VALOR TOTAL GLOBAL ESTIMADO PARA O LOTE 01							**R$ 442.641,14**	**R$ 2.773.784,68**	**R$ 12.946.047,40**

LOTE 2									
Item	**Descrição do Serviço**	**CATSER**	**Desembolso**	**Métrica ou Unidade de Medida**	**Quant. (a)**	**Valor Unitário/Mensal (b)**	**Valor Mensal (c) = (a) x (b)**	**Valor Anual (12 meses)**	**Valor Total (60 meses)**
19	Serviços de Conectividade Local	27014	mensal	unidade	30	R$ 228,61	R$ 6.858,30	R$ 82.299,60	R$ 411.498,00
20	Instalação da solução de Conectividade Local	27111	único	unidade	30	R$ 1.393,00	R$ 41.790,00	R$ 41.790,00	R$ 41.790,00
21	Treinamento da Solução de Conectividade Local	16837	único	unidade	1	R$ 12.950,00	R$ 12.950,00	R$ 12.950,00	R$ 12.950,00

VALOR TOTAL GLOBAL ESTIMADO PARA O LOTE 02	**R$ 61.598,30**	**R$ 137.039,60**	**R$ 466.238,00**

QUADRO-RESUMO DO CUSTO DA CONTRATAÇÃO	
VALOR TOTAL GLOBAL ESTIMADO PARA O LOTE 01	**R$ 12.946.047,40**
VALOR TOTAL GLOBAL ESTIMADO PARA O LOTE 02	**R$ 466.238,00**
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO →	**R$ 13.412.285,40**

1.2. Em caso de divergência entre a descrição constante do CATSER informado na tabela do item 1.1 e a descrição inserida neste Termo de Referência, prevalece a descrição do Termo de Referência.

1.3. O Lote 01 trata de Solução Integrada de Serviços Gerenciados de Firewall, Endpoints e Conectividade Wireless sob demanda e o Lote 02, de Serviço de Conectividade Local, também sob demanda.

1.4. Considerando os preços obtidos nas tabelas dos Lotes 1 e 2, o valor máximo estimado da contratação para 60 meses é de **R$ 13.412.285,40 (treze milhões, quatrocentos e doze mil duzentos e oitenta e cinco reais e quarenta centavos).**

1.4.1. Neste valor deverão estar incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

1.5. Os serviços objetos desta contratação são caracterizados como comuns, conforme justificativa apresentada pela Equipe de Planejamento da Contratação no Documento Técnico, de que possuem padrões de desempenho e qualidade que podem ser objetivamente definidos, por meio de especificações usuais no mercado, podendo ser prestado por diversos fornecedores.

1.6. O prazo de vigência dos contratos decorrentes da ata de registro de preços será de 60 (sessenta) meses, contados da data de assinatura, prorrogável, respeitando a vigência máxima de 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133/2021, desde que haja preços e condições mais vantajosas para a Administração.

1.6.1. Conforme justificativa da Equipe de Planejamento da Contratação, os serviços são enquadrados como continuados, tendo em vista serem serviços essenciais por se tratar de solução de segurança que protege os ativos de tecnologia, dados e informações existentes nos sistemas. Além disso, é contínuo por ser prestação de serviço que monitora e protege contra evolução de ameaças cibernéticas, sendo monitoramento constante de toda rede e ativos, atualização e aplicações de patches e correções para manter a proteção (seguindo as melhores práticas de conformidade e regulamentação), treinamentos e gestão de riscos, assegurando a integridade do parque tecnológico da autarquia. É um serviço que deve ser prestado constantemente, sem prazo final, devido ao fato de as soluções tecnológicas estarem enraizadas em todas as áreas das instituições, sendo parte integrante de todas as atividades executadas. A interrupção desse serviço colocaria em risco a segurança dos ativos de TI do Cofen e demais órgãos. Assim, a vigência plurianual é de sobremaneira mais vantajosa por ser uma solução robusta, de grande investimento e que as licitantes poderão diluir seu custo de investimento ao longo dos anos.

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

1.8. **Sobre a Ata de Registro de Preços**

1.8.1. Conforme art. 84 da Lei 14.133/2021 e art. 22 do Decreto 11.462/2023, o prazo de vigência da ata de registro de preços será de 1 (um) ano, contado do primeiro dia útil subsequente à data de divulgação no Portal Nacional de Contratações Públicas - PNCP.

1.8.2. O Decreto nº 11.462/2023, em seus art. 28 e 29, prevê as hipóteses de cancelamento do registro do fornecedor e de cancelamento dos preços registrados na ata de registro de preços, total ou parcialmente, desde que devidamente comprovado e justificado.

1.8.2.1. Na hipótese de cancelamento do registro do fornecedor, o Cofen poderá convocar os licitantes do cadastro de reserva, observada a ordem de classificação.

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

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, dos quais foram extraídas as especificações apresentadas abaixo, bem como as do Anexo B deste Termo de

Referência.

2.1.1. A Solução Integrada de Serviços de Segurança e de Serviços de Conectividade de Rede deverão englobar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados bem como, os serviços de monitoramento de segurança, de acordo com o lote fornecido, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.1.2. A solução deverá proporcionar disponibilidade, integridade, confidencialidade, autenticidade e segurança de todas as informações do Contratante.

2.1.3. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, em conformidade com o estabelecido no Anexo D - Níveis Mínimos de Serviço (NMS), de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

2.1.4. Os NMS serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.

2.1.5. O modelo de prestação de serviços conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo Contratante, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas periodicamente pela Contratada, tais como análise de vulnerabilidades de segurança do parque computacional do Contratante e monitoramento das ferramentas utilizadas nos serviços. Ademais, a prestação dos serviços englobará entregas que serão utilizadas, principalmente, para mensuração e verificação dos serviços realizados, tais como os relatórios de monitoramento e relatórios de resolução de problemas.

2.1.6. Em relação aos itens da tabela contida no tópico 1.1 deste Termo, temos o seguinte:

2.1.6.1. Os itens 01, 02 e 03 referem-se aos Serviços de “proteção do tráfego de rede de próxima geração” capazes de regular o tráfego de dados entre as distintas redes do Contratante e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra. Os equipamentos deverão implementar tecnologias de filtro de pacotes stateful inspection, utilizando mecanismos de verificação de tráfego segundo tabela de estado de conexões.

2.1.6.2. Os itens 04, 05 e 06 tratam dos serviços de instalação referentes aos itens A, B e C (Serviços de proteção do tráfego de rede de próxima geração, tipo A, B e C), sendo a Contratada responsável por custear todos os softwares, licenças e tudo mais que se fizer necessário tais como demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir o funcionamento de todas as funcionalidades dos serviços especificados neste Termo.

2.1.6.3. O item 7 trata de Serviços Técnicos Especializados em segurança da informação, com métrica baseada em horas de serviço, compreendendo a execução de atividades de elaboração de pareceres e planos, análise de ambiente e de ativos, auditoria forense e alteração de arquitetura do ambiente computacional e da infraestrutura de segurança do Contratante, e consiste em atividades a serem demandadas por meio da celebração prévia de ordens de serviço, com total de horas definido previamente, de comum acordo entre o Contratante e a Contratada, cujo pagamento será efetivado somente após entrega de relatório de prestação de serviços e recebimento por parte do Contratante.

2.1.6.4. Os itens 09 e 10 consistem em Serviços de “Segurança de Estações e Servidores” de forma a garantir a segurança do parque computacional do Contratante, servidores, desktops, notebooks e máquinas virtuais locais ou em nuvem, sendo de responsabilidade da Contratada todo serviço de instalação de agentes e demais softwares em todos os equipamentos necessários, a fim de garantir a segurança das informações contidas neles.

2.1.6.5. Os itens 11 e 12 tratam de “Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações e servidores” e deverá monitorar o ambiente computacional do Contratante de forma proativa, detectando e remediando as ameaças de segurança conforme especificações deste Termo.

2.1.6.6. Os itens 13 e 14 tratam dos serviços de instalação (Serviços de Segurança para proteção de estações e servidores), sendo a Contratada responsável por custear todos os softwares, licenças e tudo mais que se fizer necessário, tais como demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir o funcionamento de todas as funcionalidades dos serviços especificados neste Termo.

2.1.6.7. Os itens 8, 15, 18 e 21 tratam de treinamento.

2.1.6.8. O item 16 refere-se aos “Serviços de Conectividade Wireless”, responsável pela conectividade da

rede wireless do Contratante, possibilitando segmentação de redes corporativas e visitantes, identificação do usuário, controle de qualidade do sinal wifi e implementação de políticas de segurança para rede WAN.

2.1.6.9. O item 17 trata dos serviços de instalação da solução de Conectividade Wireless, sendo a Contratada responsável por custear todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário tais como demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir o funcionamento de todas as funcionalidades dos serviços especificados neste Termo.

2.1.6.10. O item 19: referem-se aos "Serviços de Conectividade Local", responsável pela conectividade da rede Lan do Contratante, possibilitando segmentação de redes corporativas e vlans internas.

2.1.6.11. O item 20: tratam dos serviços de instalação da solução de Conectividade Local, sendo a Contratada responsável por custear todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário tais como demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir o funcionamento de todas as funcionalidades dos serviços especificados neste Termo.

2.2. **São Características/Serviços Comuns à Solução Integrada de Segurança:**

2.2.1. Os equipamentos, produtos, peças ou softwares necessários à prestação dos Serviços de Monitoração e Administração de Segurança deverão ser instalados no ambiente do Contratante.

2.2.2. Os serviços deverão observar os seguintes requisitos mínimos, sempre que aplicável a cada uma das soluções adquiridas pelo Contratante:

2.2.2.1. Todos os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço terão o suporte em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.2.2.2. Executar as ações necessárias à resposta aos incidentes de segurança identificados de forma a manter os serviços disponíveis e operacionais.

2.2.2.3. Mapear e executar os processos de resposta dos incidentes de segurança ocorridos e documentar na base de conhecimento do Contratante.

2.2.2.4. Efetuar a manutenção das regras e políticas do parque monitorado para responder a incidentes, à exceção dos ativos sob gestão exclusiva do Contratante, cujos incidentes ou resultados de monitoração devem ser informados ao Contratante.

2.2.2.5. Verificar, diariamente, a disponibilização, pelo fabricante, de patches, correções e versões ou releases mais recentes dos softwares.

2.2.2.6. Comunicar ao Contratante a existência do patch juntamente com os respectivos problemas resolvidos e as novas funcionalidades disponibilizadas. A periodicidade dessa comunicação será definida pelo Contratante, na reunião de início do projeto (kick-off).

2.2.2.7. Atualizar os módulos da solução, isto é, fornecer e instalar patches, correções e versões ou releases mais recentes dos softwares.

2.2.2.8. Executar procedimentos, resolver problemas e esclarecer dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento dos módulos.

2.2.2.9. Executar atividades de gestão, suporte, manutenção, administração e resolução de problemas, mudanças de regras e de configuração, de cada um componentes dos serviços, remotamente ou onsite.

2.2.2.10. Realizar o ajuste fino (tunning) de toda a solução, adequando-a ao ambiente do Contratante e às customizações de configuração necessárias para atender às necessidades do Contratante.

2.2.2.11. Resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da solução.

2.2.2.12. Monitorar os sites WEB do Contratante contra pichação (defacement) e ataques, tais como cross-site scripting, SQL injection e DoS.

2.2.2.13. Monitorar servidores e alerta para mudança em arquivos de configuração.

2.2.2.14. Executar inventários contendo as informações abaixo:

a) Tipo de computador: servidor, estação ou outra classificação;

b) Sistema operacional;

c) Service pack aplicado;

d) MAC Address;

e) Portas TCP e UDP ativas.

2.2.2.15. Serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do Contratante, tais como:

a) Acessos indevidos;

b) Instalação de códigos maliciosos;

c) Indisponibilidade dos serviços (DoS e DDoS);

d) Ataques por força bruta;

e) Exploração de vulnerabilidades.

2.2.2.16. A monitoração deve utilizar canais de dados WAN próprios e redundantes com tolerância a falhas, alocados no escopo da contratação, out-of-band (sem utilizar recursos de rede WAN do Contratante dedicados a este fim, conectando a "Rede COFEN" à "Rede de Gerência" e à "Rede de Monitoração" da Contratada, com acesso restrito e por meio de conexão segura e criptografada).

2.2.2.17. Será permitida a prestação dos serviços por meio de:

a) Estabelecimento de VPN em links Internet alocados pela Contratada exclusivamente para essa conexão ou estabelecimento de VPN em links SLDD alocados pela Contratada exclusivamente para essa conexão;

b) Caso seja necessária a utilização de elementos adicionais para o estabelecimento da VPN estes devem ser alocados pela Contratada.

2.2.2.18. Avaliar periodicamente a customização dos softwares de gerência da Contratada, incluindo os alarmes de todos os componentes e ajuste das suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas no console de gerência.

2.2.2.19. Possibilidade do acesso remoto a interface de monitoramento.

2.2.2.20. Executar a gestão estratégica de cada equipamento ou software utilizado na solução, monitorando a utilização de CPU, memória e demais recursos monitoráveis, de forma a construir baseline com informações de, pelo menos, 3 (três) meses.

2.2.2.21. Deverá possuir (licitante e/ou fabricante) Centros de Operações de Segurança (SOC) redundantes, localizados no Brasil, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados. Será admitida a utilização do segundo SOC em ambiente físico terceirizado, fora das dependências da Contratada, desde que os serviços sejam prestados por funcionários da Contratada.

2.2.2.22. Caso haja elementos instalados nas dependências do Contratante, estes devem:

a) possuir fonte de alimentação 110/220V;

b) ser fixados em rack padrão 19 (sempre que aplicável).

2.3. **São Requisitos Gerais para a Prestação dos Serviços** - a Contratada deverá observar os seguintes requisitos mínimos gerais para a prestação dos serviços, sem ônus adicionais ao Contratante:

2.3.1. A Contratada será responsável por obter as assinaturas nos respectivos termos de seus funcionários, terceirizados, parceiros ou quaisquer outras pessoas que venham executar serviços integrantes do objeto desta contratação, inclusive no Modelo de Termo de Compromisso e Manutenção de Sigilo e de Ciência de Manutenção de Sigilo (Anexo G).

2.3.2. Os produtos utilizados para a prestação dos serviços devem:

2.3.2.1. estar cobertos pela garantia do fabricante durante o período de vigência de cada um dos serviços, no caso de equipamentos, produtos e peças.

2.3.2.2. estar cobertos por contratos de suporte técnico e atualização de versões junto aos fabricantes durante o período de vigência de cada um dos serviços em que serão utilizados, no caso de softwares comerciais.

2.3.3. Todos os recursos necessários à configuração e administração dos equipamentos, softwares ou quaisquer outros componentes da solução fornecida deverão ser instalados nas dependências do Contratante e estarem disponíveis mesmo com a perda de comunicação com a central de monitoramento e gerência da Contratada.

2.3.4. Quaisquer agentes ou certificados digitais necessários à perfeita consecução dos serviços devem ser alocados pela Contratada, sem ônus adicional para o Contratante.

2.3.5. A Contratada assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do Contratante ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando tenham sido causados por seus profissionais durante a execução dos serviços.

2.3.6. A Contratada deverá adotar mecanismos para proteger os equipamentos que fazem parte do escopo da solução fornecida contra roubo, furto e danos.

2.3.7. Nos equipamentos do tipo “servidor” necessários à correta prestação dos serviços deverão ser instalados produtos originais com suas respectivas licenças para funcionamento durante toda a vigência do contrato.

2.3.8. Caso o Contratante julgue pertinente, poderá ser requisitada, sem ônus adicional, a permanência da alocação dos equipamentos, softwares e demais elementos utilizados para a prestação dos serviços que tenham sido instalados nas dependências do Contratante pelo período de 03 (três) meses após o fim da vigência contratual, por meio da celebração de termo de cessão em comodato.

2.3.9. Todas as funcionalidades providas pelos equipamentos, softwares e demais elementos devem continuar ativas, sem interrupções dos serviços por eles providos, inclusive suas consoles de gerência e configuração, com exceção de:

2.3.9.1. atualização das bases de dados, incluindo de antivírus/antimalware e de reputação;

2.3.9.2. assinaturas de atualização de equipamentos;

2.3.9.3. atualização de versão de software;

2.3.9.4. prestação dos serviços de “Monitoração e Administração de Segurança”;

2.3.9.5. serviços gerenciados de segurança;

2.3.9.6. requisitos que exijam execução de atividades por parte de funcionários da Contratada;

2.3.9.7. nesse período, não será exigida prestação dos serviços de suporte, manutenção e atualização dos produtos, nem garantia do fabricante.

2.3.10. Os requisitos a seguir deverão ser atendidos por qualquer um dos itens contratados:

2.3.10.1. o acesso à administração e ao monitoramento dos ativos deverá ser realizado somente a partir da rede do Contratante ou das instalações dos SOCs e dos datacenters da Contratada/fabricante e ser realizado por meio ou protocolo seguro, com registro de acesso detalhado.

2.3.10.2. os chamados deverão ser abertos por meio de central de atendimento localizada no Brasil, a partir de número de ligação gratuita (0800) ou número local, 24 horas por dia, 7 dias por semana, ou por meio de portal na Internet.

2.3.11. Todo atendimento, do início ao encerramento do chamado, deve ser efetuado em língua portuguesa.

2.3.12. As atividades, quando realizadas no ambiente de produção, poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 18h ou em finais de semana e feriados).

2.3.13. Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema para controle de chamados da Contratada.

2.3.14. Os chamados abertos somente poderão ser fechados após autorização do Contratante.

2.3.15. A Contratada deverá realizar os devidos escalonamentos de acordo com a criticidade e nível de atendimento do incidente ou problema reportado pelo Contratante ou pelo sistema de monitoração.

2.3.16. Após resolução de um chamado técnico, a empresa Contratada deverá encaminhar ao Contratante relatório contendo descrição do chamado aberto, procedimento de resolução adotado e outros adicionais que poderão ser executados para que o problema ocorrido não se repita.

2.3.17. A Contratada deverá fornecer mensalmente, em meio magnético ou eletrônico, os relatórios abaixo descritos:

2.3.17.1. dados, informações, indicadores e métricas que permitam quantificar a quantidade de solicitações para cada tipo de chamado, incluindo os chamados abertos pela Contratada, com a média diária, semanal, mensal e anual.

2.3.17.2. dados, informações, indicadores e métricas que permitam quantificar o percentual de

disponibilidade da central de atendimento da Contratada, detalhados para a central de atendimento telefônico e para o portal na Internet.

2.3.17.3. atividades de suporte e manutenção com pelo menos descrição de: problemas, correções, aplicações de patches, mudanças de configuração e eventos ocorridos no período.

2.3.17.4. inventário lógico dos ativos.

2.3.17.5. controle de troca de equipamentos, com dados históricos de toda a duração do contrato.

2.3.17.6. chamados abertos no período, ações corretivas tomadas, tempos para execução das atividades.

2.3.17.7. relatórios analíticos contendo dados, informações, indicadores e métricas gerenciais que permitam avaliar a qualidade e o desempenho dos serviços prestados com, pelo menos, as seguintes informações:

a) utilização de CPU e memória de todos os itens;

b) utilização de recursos diversos (discos, cache, rede, etc);

c) disponibilidade de cada item;

d) atualizações de software realizadas no período;

e) total de chamados cadastrados por item;

f) classificação do chamado pelas prioridades estabelecidas;

g) tempo de atendimento por cada chamado aberto;

h) comprovação de que todos os softwares comerciais estão cobertos por contratos de suporte e atualização de versão e que todos os hardwares alocados estão cobertos por garantia do fabricante.

2.4. **Especificações Técnicas**

2.4.1. As especificações técnicas encontram-se descritas de forma detalhada no Anexo B deste Termo.

2.4.2. A solução de TIC consiste em contratação, sob demanda, de Solução Integrada de Serviços de Segurança e de Serviços de Conectividade de Rede, compreendendo: provimento de serviços de segurança de rede e endpoints; monitoramento e administração dos serviços providos; resposta a incidentes de segurança; fornecimento de solução de conectividade para rede local e wireless; instalações e configurações das soluções providas e treinamento para a equipe do Contratante, conforme tabela constante no item 1.1, com direito a atualização e suporte.

2.4.2.1. Todos os itens e quantitativos listados constituem mera expectativa em favor da Contratada, posto que depende da necessidade do Conselho, não estando o Contratante obrigado a realizá-los em sua totalidade, e não cabendo à Contratada pleitear qualquer tipo de reparação.

2.4.2.2. O Contratante não se obriga a adquirir os itens relacionados dos licitantes vencedores, nem nas quantidades indicadas neste Termo, podendo até realizar licitação específica para aquisição de um ou mais itens, nos termos do art. 83 da Lei nº 14.133/2021.

2.4.3. Conforme definido no Estudo Técnico Preliminar, a licitação será realizada em dois lotes, agrupados por itens, conforme tabela do item 1.1, visando maximizar a competividade e economicidade para o Contratante.

2.4.3.1. Os lotes foram organizados de forma a concentrar em, no máximo, duas empresas, o fornecimento dos serviços que guardam estrita relação entre si, pois é fundamental para a garantia da qualidade dos serviços que itens similares sejam fornecidos por uma mesma Contratada, visando otimizar custos e reduzir o tempo de atendimento em caso de problemas. Assim, poderá haver até duas empresas contratadas.

2.4.4. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A presente contratação justifica-se no contexto e pelos motivos abaixo descritos:

3.1.1. O Cofen, autarquia criada pela Lei nº 5.905/1973 federal, vinculada ao Ministério do Trabalho e Emprego, é órgão disciplinador do exercício da profissão de enfermeiro e das demais profissões compreendidas nos serviços de enfermagem, lidando com informações sensíveis e estratégicas.

3.1.2. O cenário atual de ameaças cibernéticas apresenta desafios crescentes para as organizações. Ataques cibernéticos sofisticados, como ransomware representam riscos significativos para a confidencialidade, integridade e disponibilidade dos dados e sistemas.

3.1.3. A infraestrutura de Tecnologia da Informação (TI) do Cofen é complexa e heterogênea, abrangendo segurança, rede de comunicação de dados, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados. Essa complexidade aumenta a superfície de ataque e dificulta a gestão eficiente da segurança da informação utilizando apenas recursos internos.

3.1.4. O Cofen vivencia uma transformação em sua área de tecnologia da informação, seja atualizando os sistemas legados, seja por demanda de novos serviços. Esse contexto demanda um ecossistema de proteção digital robusto para garantir a continuidade dos serviços, mitigar riscos de perda de informações e danos à imagem institucional, além de fortalecer a percepção de segurança perante usuários internos e a sociedade.

3.1.5. Desta forma, é essencial viabilizar a proteção adequada e atualizada do seu ambiente computacional (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de programas maléficos que ponham em risco a segurança e a continuidade das atividades.

3.1.6. Além disso, os Serviços de Conectividade de Rede permitirão aos usuários do Cofen a melhoria nas conexões à rede local e wireless, impactando também em melhorias no acesso à Internet e às aplicações publicadas em nuvem. Também farão parte do escopo atividades relacionadas à transferência de conhecimento e aos serviços técnicos especializados, segundo os requisitos mínimos elencados no Anexo B - Especificações Técnicas deste Termo.

3.1.7. Sendo assim, a contratação de Solução Integrada de Serviços Gerenciados de Segurança é essencial para prover os serviços de segurança de rede e endpoints, o monitoramento e administração dos serviços providos, a resposta a incidentes de segurança, garantindo a segurança e o controle de acesso dos usuários, à Internet e à rede local, permitindo a aplicação de filtros e a identificação de ataques externos e internos e aumentando a capacidade da equipe de segurança: a expertise e o conhecimento especializado da empresa contratada complementam as habilidades da equipe interna do Cofen, permitindo uma gestão de segurança mais eficiente e eficaz.

3.1.8. Cumpre ressaltar que a opção de contratação pela modalidade de SRP justifica-se pela conveniência em atender o Sistema Cofen/Conselhos Regionais de Enfermagem.

3.2. **Alinhamento aos Instrumentos de Planejamento Institucionais**

3.2.1. O objeto da contratação está previsto no Planejamento Orçamentário e Financeiro de 2024, conforme consta das informações deste processo.

3.2.2. O objeto da contratação está alinhado com o Planejamento Estratégico do Cofen em seu "OE06. Manter a infraestrutura física, administrativa e tecnológica do Sistema Cofen-Conselhos Regionais de Enfermagem".

3.2.3. Além disso, está em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2024 do Cofen, "Meta 01 - Contratação de solução de segurança de TIC (P22-24)" e "Meta 02 - Contratação de solução de conectividade de TIC (P22-24)".

3.3. **Parcelamento da Solução de TIC**

3.3.1. Conforme contido nos autos do presente processo, optou-se por agrupar os itens em lotes, para garantir a qualidade, eficiência e efetividade na prestação dos serviços.

3.3.2. A integração dos serviços prestados é um fator-chave a ser considerado. Ao contratar empresas para fornecer os lotes da licitação, é possível obter uma integração harmoniosa entre as atividades realizadas, facilitando a gestão dos processos e evitando problemas decorrentes de possíveis desentendimentos entre empresas contratadas. A comunicação e a colaboração entre as equipes responsáveis pela prestação dos serviços são facilitadas, resultando em maior eficiência operacional e uma melhor experiência para a Administração Pública e seus usuários.

3.3.3. Além disso, é importante destacar que distintas empresas podem apresentar divergências em relação à gestão de processos e metodologias de trabalho. A contratação de, no máximo, duas empresas evita tais disparidades, permitindo uma padronização mais efetiva dos serviços e garantindo a conformidade com os requisitos e normas estabelecidos.

3.3.4. A decisão de agrupar os itens em lotes também traz benefícios em termos de gestão de custos e recursos. Com, no máximo, duas empresas responsáveis pela prestação dos serviços, a Administração Pública pode gerir de forma mais eficiente os recursos financeiros e humanos envolvidos. Além disso, simplifica os processos de contratação e fiscalização, reduzindo a burocracia e otimizando a administração dos contratos.

3.3.5. Diante desses argumentos, torna-se essencial que a licitação para serviços seja conduzida de forma a contratar, no máximo, duas empresas para fornecer todo o objeto da licitação. Essa abordagem não apenas garante a qualidade, eficiência e efetividade dos serviços prestados, mas também proporciona uma gestão mais eficiente de custos

e recursos. O agrupamento de itens em lotes promoverá uma maior integração entre as atividades, evitando potenciais desafios de comunicação e colaboração. No final das contas, essa decisão contribuirá para o sucesso da Administração Pública em alcançar seus objetivos estratégicos e oferecer serviços de excelência aos cidadãos.

3.4. Resultados e Benefícios a Serem Alcançados

3.4.1. A solução selecionada atende aos requisitos definidos pela equipe de planejamento da contratação e da área requisitante, sendo capaz de alcançar os seguintes benefícios:

3.4.1.1. Possibilitar o atendimento aos controles e diretrizes previstas na LGPD.

3.4.1.2. Mitigação de riscos de segurança da informação associados à exposição, perdas, violações e/ou vazamentos de dados intencionais ou não por usuários do Cofen.

3.4.1.3. Diminuição de falsos positivos e negativos.

3.4.1.4. Diminuição do tratamento manual de incidentes.

3.4.1.5. Aumentar a taxa de automatização de detecção e respostas.

3.4.1.6. Melhoria da qualidade dos serviços de TIC prestados pelo Cofen à sociedade, com adoção das melhores práticas de mercado relativas à segurança da informação e comunicação.

3.4.1.7. Prevenir a ocorrência de incidentes cibernéticos que podem causar impactos à imagem e reputação do Cofen.

3.4.1.8. Alinhamento estratégico ao PDTIC, garantindo a entrega de valor para que as áreas finalísticas logrem alcançar seus objetivos específicos no âmbito da Missão Institucional do Cofen.

3.4.1.9. Ampliar o índice de confiabilidade dos usuários em relação aos serviços prestados pela área de TIC do Cofen, tendo em vista a garantia de segurança destes serviços com a implantação da solução.

3.4.1.10. Mitigar internamente os riscos de falhas na segurança dos dados institucionais, bem como identificar, investigar e tratar ocorrências, tendo em vista que a perda, roubo e/ou vazamento de dados do Órgão podem propiciar inúmeros inconvenientes e prejuízos financeiros tanto ao próprio Cofen quanto aos usuários de seus sistemas.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio:

4.1.1. Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico do Cofen, bem como disponibilização de equipamentos, bases de dados e informações precisas e confiáveis.

4.1.2. Incrementação e otimização do gerenciamento, da eficiência e da proteção das informações do ambiente tecnológico.

4.1.3. Aprimoramento continuado das ações de Segurança da Informação, objetivando o atendimento à totalidade dos usuários do ambiente tecnológico.

4.1.4. Melhoramento da capacidade de detecção e prevenção de ameaças cibernéticas, comportamentos suspeitos dos usuários, mal-uso dos dados institucionais e vazamentos de dados sensíveis.

4.1.5. Atualização e modernização do ambiente tecnológico do Cofen, mantendo assim a infraestrutura de rede segura, disponível e plenamente operacional para a disponibilidade de informações precisas e confiáveis à sociedade e aos diversos usuários de seus sistemas, assegurando deste modo o negócio.

4.2. Requisitos de Capacitação

4.2.1. Há necessidade de capacitação para a equipe do Cofen, conforme itens 8, 15, 18 e 21, se houver necessidade de ser contratado.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, ao Decreto nº 11.462/2023, à Instrução Normativa SGD/ME nº 94/2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Instrução Normativa SLTI/MPOG n° 01, de 19/01/2010, e a outras legislações aplicáveis.

4.4. Requisitos de Manutenção

4.4.1. O serviço de manutenção, atualização e suporte técnico da solução provida deverá ser executado pela

Contratada e/ou pelo fabricante durante toda a vigência contratual, a partir do Termo de Recebimento Provisório referente à implantação e operacionalização da solução no ambiente tecnológico do Cofen, e deverá contemplar obrigatoriamente no mínimo:

4.4.1.1. Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas.

4.4.1.2. Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

4.4.1.3. Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo fabricante da solução, sem ônus adicionais.

4.4.1.4. Execução de teste gerais de funcionamento e conectividade.

4.4.1.5. Execução de configuração de rede e roteamento para as aplicações configuradas.

4.4.1.6. Execução de cópia de segurança (backup) das configurações dos equipamentos.

4.4.1.7. Entrega, por parte da Contratada, de manuais técnicos e/ou documentação dos softwares licenciados em caso de alterações de tais documentos, sem ônus adicionais para o Contratante.

4.4.1.8. As novas versões do objeto deverão ser disponibilizadas pela Contratada em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão, bem como o procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados.

4.4.2. Caso os serviços de manutenção e suporte técnico não sejam executados diretamente pela Contratada, mas sim pelo próprio fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato ao Cofen e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte do Contratante do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.

4.4.3. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para o Cofen.

4.4.4. É de responsabilidade da Contratada fornecer a seus técnicos todas as ferramentas, softwares e instrumentos necessários para a execução dos serviços, bem como prover e se responsabilizar pela locomoção deles até às dependências do Contratante quando necessário.

4.5. **Requisitos Temporais**

4.5.1. Os serviços de fornecimento do objeto – isto é, a execução completa dos serviços e tarefas previstas objetivando a plena e efetiva operacionalização da solução no ambiente do Cofen – deverão ser executados no prazo máximo de até 30 dias corridos, após recebimento da Ordem de Serviço (OS) pela Contratada, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela Contratado e autorizado pelo Contratante.

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

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

4.5.4. Em caso de estabelecimento de prazos divergentes para as obrigações da contratada, deverá ser considerado o menor prazo.

4.5.5. A reunião inicial de alinhamento com a Contratada deverá ocorrer em no máximo 10 (dez) dias úteis, posteriormente à assinatura do instrumento contratual.

4.5.6. O prazo de vigência do contrato será de 60 (sessenta) meses, contados a partir da data da sua assinatura, podendo ser prorrogado, respeitada a vigência máxima decenal, desde que haja preços e condições mais vantajosas para a Administração, nos termos dos artigos 106 e 107 da Lei 14.133/2021.

4.5.7. A Contratada deve fornecer suporte técnico contínuo durante todo o período contratual. Isso inclui a disponibilidade de pessoal qualificado para responder a consultas, resolver problemas e fornecer assistência técnica de acordo com os termos estabelecidos no contrato.

4.6. **Requisitos de Segurança e Informação da Privacidade**

4.6.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante e a Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pelo Cofen para execução do Contrato.

4.6.2. A Contratada deverá executar o objeto do certame em estreita observância aos ditames estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

4.6.3. A Contratada deverá assinar Termo de Compromisso e Manutenção de Sigilo e de Ciência de Manutenção de Sigilo (Anexo G) e Termo de Compartilhamento de Dados e Confidencialidade (Anexo H), resguardando que os recursos, dados e informações de propriedade do Contratante, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

4.6.4. Não será permitido, salvo justificado, que o ambiente seguro seja acessado por pessoas da Contratada além daquelas necessárias para a prestação de serviços objeto do contrato.

4.6.5. O acesso dos profissionais da Contratada às dependências do Contrante estará sujeito às suas normas referentes à identificação (crachá funcional), trajes, trânsito e permanência em suas dependências.

4.6.6. A Contratada responsabilizar-se-á integral e solidariamente pelos atos praticados de seus empregados e/ou prestadores de serviço nas dependências do Contratante ou mesmo fora delas, que venham a causar danos ou colocar em risco o patrimônio da Contratante.

4.6.7. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pelo Contratante, incluindo as Políticas e Diretrizes de Governo, normativos associados ou específicas de Tecnologia da Informação, Política de Segurança da Informação e Comunicações e Normas Complementares do GSI/PR.

4.6.8. Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia e gerenciamento do prestador de serviços.

4.6.9. A Contratada deverá credenciar, junto ao Contratante, seus profissionais autorizados a operar presencialmente (on-site) no sítio do Contratante e, quando couber, também aqueles que terão acesso aos sistemas corporativos.

4.6.10. Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.

4.6.11. Devem ser mantidos registros sobre todas as falhas ocorridas e sobre todas as manutenções executadas.

4.6.12. A Contratada se compromete a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.

4.6.13. A Contratada deverá realizar e apresentar ao Contratante, quando solicitado, uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados ao objeto da contratação, indicando o nível de risco sob o qual o Contratante está exposto, baseada em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada por este Contratante.

4.6.14. Quando for o caso, a propriedade intelectual e os direitos autorais dos dados e informações armazenados nos bancos de dados do Contratante, hospedados na Contratada, e qualquer tipo de trabalho relacionado às demandas do Contratante, serão de sua titularidade, nos termos do artigo 4º da Lei nº 9.609/1998.

4.6.15. A Contratada deverá garantir a segurança das informações do Contratante e deverá se comprometer a não divulgar ou repassar a terceiros qualquer informação que tenha recebido do Contratante, a menos que autorizado formalmente e por escrito para tal.

4.6.16. A Contratada deverá reportar imediatamente ao Contratante incidentes que envolvam vazamento de dados, fraude ou comprometimento da informação relacionados ao objeto do contrato.

4.6.17. Sempre que solicitado, a Contratada deverá fornecer ao Contratante toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados, a fim de assegurar a auditoria da solução Contratada, bem como demais dispositivos legais aplicáveis.

4.6.18. Toda informação confidencial disponível em razão desta contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses:

4.6.18.1. Término ou rompimento do Contrato;

4.6.18.2. Solicitação do Contratante.

4.7. **Requisitos Sociais, Ambientais e Culturais**

4.7.1. Durante a execução de tarefas no ambiente do Contratante, os colaboradores da Contratada deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, conforme as normas internas da instituição.

4.7.2. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo Conselho.

4.7.3. A Contratada deverá atender, quando da execução do objeto do contrato, os critérios de sustentabilidade ambiental previstos na legislação pertinente, quando couber.

4.7.4. As configurações de hardware e software deverão ser executadas visando alto desempenho com o uso racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos.

4.7.5. Toda a documentação produzida e/ou fornecida pela Contratada referente ao objeto deverá estar preferencialmente no idioma português do Brasil (pt-BR), de forma clara e objetiva.

4.8. **Requisitos da Arquitetura Tecnológica**

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

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

4.8.3. Durante a implantação da solução, a Contratada deverá realizar, de acordo com o lote fornecido, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

4.8.4. Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.

4.8.5. Caberá à Contratada a disponibilização de ferramentas/scripts de retorno imediato ao estado original da estrutura do Contratante, caso a instalação e migração dos hardwares/softwares da Contratada apresente falha.

4.8.6. A Contratada realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.

4.8.7. A Contratada deverá fornecer todas as licenças necessárias de todos os componentes da solução ofertada e dos elementos adicionais que se fizerem necessários à instalação/migração e à perfeita operação do ambiente de produção.

4.8.8. Outros detalhes técnicos acerca da Solução de TIC a ser contratada encontram-se no Anexo B - Especificações Técnicas deste Termo.

4.9. **Requisitos de Projeto e de Implementação**

4.9.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do Contratante em no máximo 30 (trinta) dias corridos, após recebimento da Ordem de Serviço (OS) pela Contratada.

4.9.2. Em caso de alterações necessárias nas especificações do projeto original durante a execução dos trabalhos, competirá à Contratada elaborar o projeto da parte a ser alterada e submetê-lo à aprovação do Fiscal, não podendo ocorrer, no entanto, alteração substancial das disposições gerais formuladas pelo projeto original.

4.9.3. A Contratada deverá fornecer ao Contratante a documentação contendo as especificações técnicas detalhadas dos produtos oferecidos.

4.10. **Requisitos de Implantação**

4.10.1. Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

4.10.1.1. responsabilizar-se pela completa implantação do projeto, ou seja, por todos os custos e providências necessárias à operacionalização dos equipamentos.

4.10.1.2. responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes

de aceitação.

4.10.1.3. instalar e configurar todos os produtos do fornecimento da solução.

4.10.1.4. executar a integração de todos os produtos da solução, de acordo com o lote fornecido, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega.

4.10.1.5. elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e/ou gerencial.

4.10.1.6. realizar um mapeamento completo e uma verificação dos dados de gestão existentes. Isso envolve assegurar que todas as informações relevantes estejam corretamente identificadas e associadas aos produtos e licenças correspondentes.

4.10.1.7. deverá garantir que as informações de gestão já existentes sejam corretamente integradas e mantidas. Isso envolve a sincronização das licenças adquiridas no novo contrato com as informações de gestão existentes, caso pertinente.

4.11. **Requisitos de Garantia e Manutenção**

4.11.1. Os itens que compõe a solução deverão ter garantia durante toda a vigência contratual.

4.11.2. O acesso para downloads de patches, drivers e quaisquer outras atualizações e/ou correções necessárias devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de garantia técnica, e podem ser feitos através de http ou ftp, no sítio do fabricante da solução.

4.11.3. Caso o contrato seja renovado, a garantia também será renovada, de acordo com as quantidades, requisitos e especificações constantes no documento.

4.12. **Requisitos de Experiência Profissional**

4.12.1. A equipe responsável pela execução do objeto deve ser composta por profissionais qualificados e capacitados, de acordo com os requisitos estabelecidos. A qualificação da equipe é de extrema importância para garantir a excelência na prestação dos serviços e a obtenção dos resultados esperados.

4.13. **Requisitos de Formação da Equipe**

4.13.1. A Contratada deverá apresentar em até 30 (trinta) dias após a assinatura do contrato pelo menos um técnico certificado na solução proposta.

4.14. **Requisitos de Metodologia de Trabalho**

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

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

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

4.14.4. A Contratada deve adotar uma abordagem centrada no cliente, priorizando o entendimento das necessidades e requisitos específicos da organização contratante. É importante que a CONTRATADA seja capaz de oferecer orientações adequadas às necessidades do Conselho, levando em consideração fatores como tamanho, tipo de negócio e orçamento disponível.

4.14.5. A Contratada deve oferecer suporte técnico adequado para auxiliar a organização contratante na instalação, configuração e solução de problemas, bem como é obrigatório que a Contratada possua uma equipe de suporte qualificada, capaz de lidar com consultas e problemas técnicos de maneira eficiente e eficaz.

4.15. **Vistoria**

4.15.1. A avaliação prévia do local de execução dos serviços é facultativa e tem por objetivo dar conhecimento pleno das condições e peculiaridades do objeto a ser contratado ao Contratante, além de garantir que todos as licitantes conhecem integralmente o objeto da licitação e, por consequência, que suas propostas de preços possam refletir com exatidão a sua plena execução, evitando-se futuras alegações de desconhecimento das características do objeto licitado, resguardando o Contratante de possíveis inexecuções contratuais.

4.15.2. Para as licitantes que optarem pela não realização da vistoria, não serão aceitas alegações posteriores quanto ao detalhamento, especificações e obrigações que compõe esta contratação, ficando a futura Contratada obrigada

a executar o contrato nos termos dispostos neste Termo de Referência e seus apêndices.

4.15.2.1. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.15.3. A vistoria deverá ser previamente agendada pela licitante com o unidade de Tecnologia da Informação e Comunicação do Contratante através dos telefones de contato constantes no Anexo A e deverá, obrigatoriamente, ser realizada por representante da licitante que tenha condições técnicas suficientes para identificar com clareza os recursos necessários que deverão ser utilizados no objeto da licitação em comento, de forma a possibilitar a correta formulação da proposta comercial a ser apresentada na sessão pública.

4.15.4. O representante da licitante designado para realizar a vistoria prévia de que trata este item, deverá apresentar ao Contratante, no momento da vistoria, documento oficial de identificação, bem como autorização emitida pelo licitante para a realização de vistoria.

4.15.5. A vistoria prévia deverá ser realizada no período compreendido entre a data da publicação do Edital e o último dia útil anterior à sessão pública do processo licitatório, das 9h às 12h e das 14h às 17h, na sede do Contratante, conforme os endereços constantes no Anexo A.

4.15.6. Ao final da vistoria prévia acima mencionada o representante da licitante deverá assinar a Declaração de Vistoria, a qual será juntado aos autos.

4.15.7. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia. Não haverá vistoria sem prévio agendamento e em mesma data/horário por mais de uma licitante tampouco no dia da sessão pública.

4.16. **Sustentabilidade**

4.16.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos, no que couber, os requisitos que se baseiam no Guia Nacional de Contratações Sustentáveis e na IN SLTI/MP nº 01/2010 que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratações de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional.

4.16.2. Deverão ser estimuladas as boas práticas de otimização de recursos, redução de desperdícios e menor poluição pautados nos seguintes pressupostos e exigências, quando couberem:

4.16.2.1. Fazer uso racional de água, adotando medidas para evitar o desperdício de água tratada e mantendo critérios especiais e privilegiados para aquisição e uso de equipamentos e complementos que promovam a redução do consumo.

4.16.2.2. Economia de energia.

4.16.2.3. Reciclagem de lixo.

4.16.2.4. Repassar a seus empregados todas as orientações referentes à redução do consumo de energia e água.

4.16.3. A licitante vencedora deverá respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos e outras pertinentes.

4.16.4. Além do apontado acima, devem ser observadas pela Contratada outras práticas sociais, devendo comprovar, como condição prévia à assinatura do contrato e durante a vigência contratual, sob pena de rescisão contratual, o atendimento das seguintes condições:

4.16.4.1. Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas à escravidão, instituído pela Portaria Interministerial MTPS/MMIRDH nº 04 de 11/05/2016;

4.16.4.2. Não ter sido condenada, a Contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988, do art. 149 do Código Penal Brasileiro, do Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nº 29 e 105.

4.17. **Da Exigência de Carta de Solidariedade**

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

4.18. **Subcontratação**

4.18.1. Não é admitida a subcontratação do objeto contratual.

4.19. **Da Verificação de Amostra do Objeto**

4.19.1. A licitante classificada provisoriamente em primeiro lugar que tiver sua proposta de preços aceita e a documentação de habilitação aprovada poderá, a critério do Contratante, ser convocada para executar prova de conceito, conforme as regras estabelecidas no Anexo C - Prova Conceito deste Termo.

4.20. **Garantia da Contratação**

4.20.1. Será exigida a garantia da contratação correspondente a 2% (dois por cento) do total do Contrato, de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021.

4.20.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.20.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 20 dias úteis após a assinatura do contrato.

4.20.4. A garantia será utilizada para reparar danos decorrentes das ações ou omissões da Contratada, para o pagamento de eventuais multas e, ainda, para satisfazer qualquer obrigação, judicial ou extrajudicial, resultante ou decorrente de suas ações ou omissões.

4.20.5. A Contratada se compromete a manter a garantia no valor correspondente ao percentual fixado, durante toda a vigência do Contrato, ficando obrigado a integralizá-lo, no prazo de 10 (dez) dias úteis, sempre que houver acréscimo no valor do Contrato ou utilização parcial/integral da garantia pela Contratante.

4.20.6. A garantia prestada pela Contratada será restituída após a quitação integral das obrigações contratuais.

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

4.21. **Informações relevantes para o dimensionamento e apresentação de proposta**

4.21.1. A demanda do Cofen tem como base as informações levantadas pelo DTIC/Equipe de Planejamento da Contratação que estão dispostas ao neste documento e em seus anexos.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações do Contratante:

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos.

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência.

5.1.3. Receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos e condições preestabelecidos em contrato.

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável.

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.1.9. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

5.1.10. Exercer o acompanhamento e a fiscalização dos serviços, por funcionário (ou comissão) especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências

cabíveis.

5.1.11. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas.

5.1.12. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto.

5.1.13. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento.

5.1.14. Proporcionar todas as facilidades para que a Contratada possa cumprir suas obrigações dentro das normas e condições contratuais.

5.1.15. Permitir ao pessoal da Contratada livre acesso às dependências do Contratante, de modo a viabilizar a prestação dos serviços durante o horário de expediente do órgão, ou fora dele, quando solicitado e/ou autorizado pelo Fiscal do Contrato.

5.1.16. Aplicar as penalidades previstas em contrato, quando for o caso, assegurando o contraditório e a ampla defesa à Contratada.

5.1.17. É vedado ao Contratante praticar atos de ingerência na administração da Contratada.

5.2. São obrigações da Contratada:

5.2.1. Indicar formalmente preposto apto a representá-la junto ao contratante, que deverá responder pela fiel execução do contrato.

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

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

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

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

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

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

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

5.2.9. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do Contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

5.2.10. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

5.2.11. Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa para garantir a qualidade do atendimento às especificações contidas neste Termo, no Edital e em seus Anexos.

5.2.12. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, pelo desempenho, pela eficiência e pela produtividade, com fins para a execução dos trabalhos, dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas.

5.2.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação.

5.2.14. Arcar com todos os encargos sociais e trabalhistas, previstos na legislação vigente, e de quaisquer outros

em decorrência da sua condição de empregadora, no que diz respeito aos seus colaboradores.

5.2.15. Informar ao Cofen, no prazo de 48 (quarenta e oito) horas, qualquer alteração social ou modificação da finalidade ou estrutura da empresa.

5.2.16. Manter a mais absoluta confidencialidade a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, dispositivos, modelos, bases de dados ou outros materiais de propriedade do Cofen ou de terceiros, aos quais tiver acesso em decorrência da prestação de serviços para o objeto do contrato, ficando terminantemente proibida de fazer uso ou revelar estes, sob qualquer justificativa.

5.2.17. Prestar todos os esclarecimentos e informações que forem solicitados pelo Contratante, de forma clara, concisa e lógica, atendendo de imediato às reclamações, inclusive relatando qualquer problema que possa impactar o andamento dos serviços ou o cumprimento dos níveis de serviço deve ser imediatamente comunicado ao Contratante, garantindo ao Contratante, a qualquer tempo, acesso aos documentos relativos à execução dos serviços.

5.2.18. Levar, imediatamente, ao conhecimento do fiscal do contrato do Cofen, qualquer fato extraordinário ou anormal que ocorrer na execução do objeto contratado, para adoção das medidas cabíveis.

5.2.19. Executar os serviços conforme especificações do edital e seus anexos e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, se for o caso, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta.

5.2.20. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

5.2.21. Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal na execução dos serviços.

5.2.22. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

5.2.23. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

5.2.24. Conduzir os trabalhos com estrita observância à legislação e normas pertinentes, cumprindo as determinações dos poderes públicos e as normas de segurança do Contratante.

5.2.25. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

5.2.26. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

5.3. São obrigações do órgão gerenciador do registro de preços:

5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3.1. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.3.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.4.1. A definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

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

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

6. MODELO DE EXECUÇÃO DO OBJETO

6.1. Condições de execução

6.1.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1.1. A reunião inicial de alinhamento com a Contratada deverá ocorrer em no máximo 10 (dez) dias úteis, posteriormente à assinatura do instrumento contratual.

6.1.1.2. Caso seja necessário, Contratante e Contratada poderão realizar outras reuniões, com a finalidade de ajustar a execução dos serviços, entre os gestores do contrato e o preposto da Contratada, registrando os acordos em ata. A elaboração dessas atas são responsabilidade do preposto da Contratada.

6.1.1.3. A Contratada deverá elaborar cronograma com data prevista de início e fim de todas as fases respeitando os prazos estipulados neste Termo.

6.1.1.4. O início da execução do objeto se dará imediatamente após recebimento da ordem de serviço pela Contratada, ocasião em que deverá ser apresentado cronograma da execução do serviço.

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

6.1.1.6. Todo e qualquer serviço somente será executado mediante abertura prévia de Ordem de Serviço (OS) emitida pelo Contratante.

6.1.1.7. As Ordens de Serviço terão seu layout definido pelo Contratante após a contratação e dela constarão todas as especificações necessárias para o registro, o ateste, a entrega e avaliação dos produtos/serviços.

6.1.1.8. Nos casos excepcionais, em que a Contratada não consiga executar a Ordem de Serviço, conforme as condições demandadas, por motivos de dependência de alguma ação da própria do Contratante ou por motivos de força maior, deverá comunicar ao Fiscal Técnico do Contrato por escrito e com antecedência, justificando os fatos e motivos que impedirão sua execução, cabendo ao Fiscal avaliar a admissibilidade das justificativas.

6.1.1.9. Qualquer dificuldade durante a prestação dos serviços deve ser imediatamente reportada ao Contratante, sob risco de não ser aceita a alegação de culpa de terceiros, como justificativa para execução inadequada, insatisfatória ou incompleta dos serviços.

6.1.1.10. Depois de identificadas as demandas, o Fiscal do Contrato encaminhará a OS para a Contratada, bem como as informações necessárias para análise da demanda.

6.1.1.11. A OS será precisa e contemplará o detalhamento do serviço, as atividades previstas, os padrões a serem seguidos, bem como demais informações técnicas necessárias para a execução dos serviços por parte da Contratada.

6.1.1.12. Qualquer alteração nas definições descritas na OS deverá gerar uma nova Ordem de Serviço complementar, fazendo referência à anterior que originou os serviços.

6.1.1.13. A Contratada deverá entregar os produtos demandados, de acordo com os respectivos cronogramas e dentro dos padrões de qualidade e de compatibilidade técnica, conforme as definições deste Termo de Referência.

6.2. Local e horário da prestação dos serviços

6.2.1. Os serviços serão prestados nos endereços constantes no Anexo A. Eventualmente, o endereço de entrega poderá ser alterado, desde que seja dentro da mesma cidade e informado previamente à Contratada.

6.2.2. Os serviços serão prestados em período integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

6.2.3. Será de inteira responsabilidade da Contratada assegurar a prestação dos serviços durante os horários definidos pelo Contratante.

6.3. Materiais a serem disponibilizados

6.3.1. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar, no mínimo, os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades estabelecidas neste Termo de

Referência, promovendo sua substituição quando necessário.

6.4. **Especificação da garantia do serviço**

6.4.1. O prazo de garantia contratual para todos os serviços, complementar à garantia legal, será de 60 (sessenta) meses, diretamente pelo fabricante ou empresa autorizada por ele.

6.5. **Formas de Transferência de Conhecimento e Procedimentos de Transição e Finalização do Contrato**

6.5.1. Serão necessários procedimentos de transição e finalização do contrato. Tais procedimentos visam não deixar lacuna entre durante o período final dos serviços executados pela então atual Contratada e uma nova Contratada.

6.5.2. A Contratada deverá permitir renovação das licenças ao final do contrato inicial. A Contratada deve estar preparada para gerenciar esse processo de renovação e garantir que seja concluído dentro do prazo estabelecido.

6.5.3. Deve ser observado o previsto nos itens 5.2.9 deste Termo e o inciso XI, alínea "c", do item 2.8.1.3 do Anexo B - Especificações Técnicas.

6.6. **Mecanismos formais de comunicação**

6.6.1. São definidos como mecanismos formais de comunicação, entre o Contratante e a Contratada, os seguintes:

a) Ordem de Serviço e/ou Fornecimento;

b) Ata de Reunião;

c) Ofício;

d) Sistema de abertura de chamados;

e) E-mails.

6.6.2. O canal de comunicação entre o Contratante e a Contratada para assuntos relacionados à gestão e fiscalização contratual, ocorrerá preferencialmente através da figura do preposto. O preposto é o representante da Contratada junto ao Contratante. O preposto poderá ser contatado mesmo fora do horário de expediente, sem que com isso ocorra qualquer ônus extra para o Contratante.

6.6.3. A comunicação entre o Contratante e a Contratada se dará preferencialmente por meio escrito, sempre que se entender necessário o registro de ocorrência relacionada com a execução do contrato.

6.7. **Formas de Pagamento**

6.7.1. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6.7.2. Os critérios de medição e pagamento dos serviços prestados serão tratados tópicos próprios do "Modelo de Gestão do Contrato" e "Critérios de Medição e Pagamento".

6.8. **Manutenção de Sigilo e Normas de Segurança**

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

6.8.2. O Termo de Compromisso de Manutenção de Sigilo e de Ciência de Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e o Termo de Ciência de Manutenção de Sigilo e das normas de segurança, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se unificados no Anexo G, em atendimento ao artigo 18, inciso V, alíneas “a” e “b” da Instrução Normativa SGD/ME nº 94, de 2022, previstos para contratações que envolvem a prestação de serviços de TIC.

7. MODELO DE GESTÃO DO CONTRATO

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

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

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato

exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

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

7.5. **Preposto**

7.5.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

7.5.2. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

7.6. **Reunião Inicial**

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

7.6.2. A reunião será realizada em conformidade com o previsto no inciso I do art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério do Contratante.

7.6.3. A pauta desta reunião observará, pelo menos:

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

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

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

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

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

7.7. **Fiscalização**

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

7.7.2. A fiscalização de que trata este item será exercida no interesse do Contratante e não exclui, nem reduz a responsabilidade da Contratada por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior.

7.8. **Fiscalização Técnica**

7.8.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.8.4. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

7.9. **Fiscalização Administrativa**

7.9.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.9.2. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.10. **Gestor do Contrato**

7.10.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.10.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.10.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da Contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.10.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pela Contratada, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.10.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133/2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.10.6. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

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

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o disposto neste item para aferição da qualidade da prestação dos serviços, sem prejuízo da aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

8.2. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pelo Contratante, terão tratamento conforme tabela abaixo:

ID	OCORRÊNCIA	GLOSA/SANÇÃO
1	Não prestar os esclarecimentos, de forma imediata, referente à execução do objeto, salvo quando se tratarem de indagações de caráter técnico, hipótese em que deverão ser respondidos em até 72 horas úteis.	Multa de 0,5% do valor total fatura mensal por dia de atraso, até o limite de 5 dias úteis.
		Após o limite de 5 dias úteis, será aplicada, cumulativamente, multa de 2% do valor total da fatura mensal.
2	Não atender ao Indicador de Nível de Serviço IAP (índice de atendimento no prazo)	IAP>=90%: sem aplicação de penalidade
		IAP >=80% e <90%: multa de 0,5% sobre o valor total da fatura mensal.
		IAP >=70% e <80%: multa de 1% sobre o valor total da fatura mensal.
		IAP <70%: multa de 2% sobre o valor total da fatura mensal.
3	Não implementar o objeto no prazo estipulado neste Termo de Referência	Multa de 0,5% do valor total do contrato por dia de atraso, até o limite de 30 dias.
		Após o limite de 30 dias, será aplicada, cumulativamente, multa de 20% sobre valor total do contrato, podendo acarretar na sua rescisão.

4	Deixar de cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplicar-se-á multa de 10% sobre o valor total do contrato.

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

8.3.1. não produzir os resultados acordados;

8.3.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

8.3.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8.4. O objeto terá sua qualidade aferida periodicamente, obedecendo o disposto neste Termo, e ainda, observará o cumprimento de todos os prazos, obrigações contratuais e os critérios de qualidade e adequação estabelecidos pelo Contratante.

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

8.5.1. Aprovação de medição mensal pelos fiscais do contrato, mediante apresentação de relatório com aferição dos indicadores de qualidade dos serviços prestados para avaliação do Contratante. Somente após aprovação do relatório pelo fiscal do contrato, a Contratada poderá emitir a Nota Fiscal.

8.5.2. Entrega de certidões e demais documentos de comprovação de regularidade fiscal e trabalhista;

8.5.3. Entrega de comprovação de entrega de materiais, insumos e equipamentos necessários para a execução do serviço;

8.5.4. Entrega de demais documentos solicitados pela fiscalização com a devida justificativa.

8.6. **Do Recebimento**

8.6.1. Todos os serviços/itens serão recebidos provisoriamente, no prazo de até 10 (dez) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

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

8.6.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.6.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

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

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

8.6.5.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

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

8.6.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.6.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis. Nos termos do art. 140, §4º, da Lei 14.133/21, salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução

do objeto do contrato exigidos por normas técnicas oficiais correrão por conta da Contratada.

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

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

8.6.11. Os serviços/itens 1, 2, 3, 11, 12, 16, 19 serão recebidos definitivamente no prazo de até 20 (vinte) dias e os demais serviços/itens (4, 5, 6, 7, 8, 9, 10, 13, 14, 15, 17, 18, 20 e 21) no prazo de até 10 (dez) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.6.11.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

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

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

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

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

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

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

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

8.6.15. O processo de recebimento dar-se-á nos termos da IN SGD/ME nº 94, de 2022 regido pela Lei nº 14.133/2021 e eventuais atualizações, seguindo o diagrama ilustrativo do processo de "Execução da OS/OFB" disponibilizado no link *https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/execucao-da-os-ofb.png*

8.6.15.1. Este diagrama poderá sofrer adaptações a critério do Contratante, em vista de mudanças operacionais e administrativas que venham a ocorrer em seu ambiente, sempre de acordo com a legislação vigente.

8.7. **Procedimentos de Teste e Inspeção**

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

8.7.1.1. verificação da adequação da solução de TIC às especificações funcionais e tecnológicas;

8.7.1.2. inspeção e avaliação da solução por amostragem ou total do fornecimento de bens ou da prestação de serviços;

8.7.1.3. adoção de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores estabelecidos;

8.7.1.4. definição de listas de verificação e de roteiros de testes para subsidiar a ação dos fiscais do contrato;

8.7.1.5. previsão de inspeções e diligências, quando aplicáveis, e suas formas de exercício.

8.7.2. A realização de testes não isenta a Contratada de corrigir os defeitos que vierem a ser encontrados mesmo após a realização dos testes e ateste pelo Contratante.

8.7.3. A realização dos testes pelo Contratante não exime a Contratada da responsabilidade de efetuar os devidos testes antes da entrega, a fim de garantir os padrões mínimos de qualidade exigidos e entregar a solução ao Contratante livre de erros.

8.7.4. A homologação do Contratante e aceite definitivo do objeto estão condicionados ao atendimento dos seguintes requisitos:

8.7.4.1. Pleno atendimento às especificações funcionais e técnicas;

8.7.4.2. Adequação às necessidades do usuário;

8.7.4.3. Total integração com os sistemas já existentes, se for o caso;

8.7.4.4. Base de dados totalmente convertida, se houver necessidade de migração de dados;

8.7.4.5. Solução livre de erros nos testes realizados;

8.7.4.6. Documentação completa, escrita em português, como falado no Brasil;

8.7.5. Os prazos estabelecidos para conclusão dos serviços não serão alterados em função das devoluções por problemas de qualidade, descontando-se tão somente o tempo gasto pelo Contratante para análise dos produtos.

8.8. **Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento**

8.8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021 e cada parte responderá pelas consequências de sua inexecução total ou parcial. A aplicação das sanções obedecerá ao disposto nos artigos 155 a 163 da Lei nº 14.133/2021.

8.8.2. A Contratada será responsabilizada administrativamente pelas infrações que cometer, estando sujeita às sanções administrativas previstas no artigo 155 e seguintes da Lei nº 14.133/2021.

8.8.3. Comete infração administrativa o fornecedor que praticar quaisquer das hipóteses previstas no art. 155 da Lei nº 14.133/2021, quais sejam:

8.8.3.1. Dar causa à inexecução parcial do contrato;

8.8.3.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.8.3.3. Dar causa à inexecução total do contrato;

8.8.3.4. Deixar de entregar a documentação exigida para o certame;

8.8.3.5. Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;

8.8.3.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

8.8.3.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

8.8.3.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

8.8.3.9. Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

8.8.3.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

a) Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

8.8.3.11. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

8.8.3.12. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

8.8.4. Pelo cometimento de qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

8.8.4.1. Advertência pela falta do subitem 8.8.3.1 deste Termo de Referência, quando não se justificar a imposição de penalidade mais grave;

8.8.4.2. Multa por qualquer das infrações dos subitens 8.8.3.1 a 8.8.3.12;

a) As multas aqui previstas, no caso de atraso injustificado, assim considerado pela Administração, inexecução parcial ou inexecução total da obrigação, sem prejuízo das responsabilidades civil e criminal,

assegurada a prévia e ampla defesa, serão aplicadas nos seguintes termos:

b) 0,5% (cinco décimos por cento) por dia sobre o valor contratado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

c) 0,7% (sete décimos por cento) até 10% (dez por cento) sobre o valor contratado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumidas.

d) 0,8% (oito décimos por cento) até 15% (quinze por cento) sobre o valor contratado, em caso de inexecução total da obrigação assumida.

8.8.4.3. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.8.3.2 a 8.8.3.7 deste Termo de Referência, quando não se justificar a imposição de penalidade mais grave;

8.8.4.4. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.8.3.8 a 8.8.3.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

8.8.5. A aplicação das sanções previstas neste Termo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.8.7. Antes da aplicação da multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante à Contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.8.9. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.8.11. Na aplicação das sanções serão considerados:

8.8.11.1. a natureza e a gravidade da infração cometida;

8.8.11.2. as peculiaridades do caso concreto;

8.8.11.3. as circunstâncias agravantes ou atenuantes;

8.8.11.4. os danos que dela provierem para o Contratante;

8.8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.8.12. Os atos previstos como infrações administrativas na Lei nº 14.133/2021 ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013 serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.8.13. A personalidade jurídica da Contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo ou para provocar confusão patrimonial e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.8.14. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção,

informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

8.8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021.

8.8.16. O descumprimento do pactuado na ata de registro de preço ensejará aplicação das penalidades estabelecidas no edital, sendo da competência do gerenciador a aplicação das penalidades.

8.8.17. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

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

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

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

8.9. **Liquidação**

8.9.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77 /2022.

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

8.9.3. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;

b) a data da emissão;

c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) o valor a pagar; e

f) eventual destaque do valor de retenções tributárias cabíveis.

8.9.4. A Contratada lançará na Nota Fiscal as especificações do objeto contratado de modo idêntico àquelas constantes no Termo de Contrato.

8.9.5. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.9.6. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133 /2021.

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

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

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

recebimento de seus créditos.

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

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

8.10. **Prazo de pagamento**

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

8.10.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo da Tecnologia da Informação (ICTI) de correção monetária.

8.11. **Forma de pagamento**

8.11.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada.

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

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

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

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

8.12. **Reajuste**

8.12.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

8.12.2. Após o interregno de um ano, desde que solicitado pela Contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.12.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.12.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s), ficando a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

8.12.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

8.12.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

8.12.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

8.12.8. O reajuste será realizado por apostilamento.

8.13. **Cessão de crédito**

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

8.13.1.1. As cessões de crédito não abrangidas pela Instrução Normativa SEGES/ME nº 53, de 8 de julho de

2020 dependerão de prévia aprovação do Contratante.

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

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

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

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

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO POR LOTE, via SISTEMA DE REGISTRO DE PREÇOS.

9.1.2. O SRP será adotado por se enquadrar na hipótese prevista no inciso III do art. 3º do Decreto nº 11.462/23, conforme transcrição abaixo:

> "III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas"

9.1.3. A opção de contratação pela modalidade de Sistema de Registro de Preços justifica-se pela conveniência em atender o Sistema Cofen/Conselhos Regionais de Enfermagem e, eventualmente, outros órgãos da administração.

9.1.4. O Conselho Federal de Enfermagem – Cofen será o Órgão Gerenciador, sendo, portanto, o responsável pela condução da licitação e gerenciamento da Ata de Registro de Preços.

9.1.5. O registro de preços será formalizado através de Ata de Registro de Preços, na forma da minuta constante em edital e nas condições previstas neste Termo. A Ata de Registro de Preços terá efeito de compromisso de fornecimento, ficando os fornecedores nela incluídos obrigados a celebrar as ordens de fornecimento ou contratos que advierem nas condições estabelecidas neste Termo de Referência.

9.1.6. Deverá ser divulgado a Intenção de Registro de Preços (IRP), em conformidade com o art. 9 do Decreto nº 11.462/23, possibilitando, pelo prazo mínimo de oito dias úteis, a participação de outros órgãos ou outras entidades da Administração Pública na ata de registro de preços e determinando a estimativa total de quantidades da contratação.

9.1.7. Será permitida a adesão à Ata de Registro de Preços por órgãos não partícipes para possibilitar que todos os Conselho Regionais de Enfermagem façam a adesão, caso decidam pela contratação posteriormente à fase de Intenção de Registro de Preços (IRP).

9.2. Regime de execução

9.2.1. O regime de execução do contrato será por preço unitário.

9.3. Da Aplicação da Margem de Preferência

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

9.4. Exigências de habilitação: para fins de habilitação, deverá o licitante comprovar os seguintes requisitos, quando aplicável:

9.4.1. Habilitação jurídica

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

9.4.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual -

CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

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

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

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

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

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

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

9.4.1.9. Fica vedada a participação de:

a) Pessoa Física: entende-se, conforme parágrafo único, do art. 4º, da IN 116/2021, que a contratação exige estrutura mínima para realização de entrega, equipe de técnicos certificados para a instalação, operação e treinamento, o que é incompatível com a natureza profissional da pessoa física.

9.4.1.10. A pessoa jurídica poderá participar de licitação em consórcio, desde que observadas as seguintes normas, bem como o contido nos arts. 15 e 67 da Lei 14.133/21 e as demais disposições do edital sobre o tema:

I - comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

II - indicação da empresa líder do consórcio, que será responsável por sua representação perante a Administração;

III - admissão, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

IV - impedimento de a empresa consorciada participar, na mesma licitação, de mais de um consórcio ou de forma isolada;

V - responsabilidade solidária dos integrantes pelos atos praticados em consórcio, tanto na fase de licitação quanto na de execução do contrato.

9.4.2. **Habilitação fiscal, social e trabalhista**

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

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

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

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

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

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

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

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

9.4.3. **Qualificação Econômico-Financeira**

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

9.4.3.2. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

9.4.3.3. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

b) as empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

c) os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

d) os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

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

9.4.3.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

9.4.3.6. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo licitante, a fim de se garantir maior segurança à Administração, evitando-se eventuais riscos de incapacidade econômica do licitante em suportar as suas obrigações constantes no certame, em conformidade com a previsão do § 1º do art. 69 da Lei nº 14.133/2021.

9.4.4. **Qualificação Técnica**

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

a) A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

9.4.4.2. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado. Para fins da comprovação de que trata este item, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

a) Ao menos 1 (um) atestado de capacidade técnica expedido por pessoa jurídica de direito público ou privado, em nome da licitante, que comprove a execução de serviço compatível com o objeto da licitação, com a comprovação de aptidão para implantação e operação de Solução Integrada de Serviços de Segurança e de Serviços de Conectividade de Rede, compreendendo os itens de maior relevância, a saber: itens 1 (Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A), 2 (Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo B), 3 (Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C), 7 (Serviços Técnicos Especializados), 9 (Serviços de

Solução de proteção para Estações), 10 (Serviços de Solução de proteção para Servidores), 11 (Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações), 12 (Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para servidores), 16 (Serviços de Conectividade Wireless) e 19 (Serviços de Conectividade Local), em características, quantidades e prazos compatíveis, comprovando que a licitante executa ou executou contrato correspondente a 50% (cinquenta por cento) da quantidade estimada dos referidos itens para a presente contratação.

9.4.4.3. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

9.4.4.4. Os atestados apresentados deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente da licitante.

9.4.4.5. Os atestados devem estar emitidos para o CNPJ da licitante. Não serão admitidos atestado relativos ao grupo econômico.

9.4.4.6. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

9.4.4.7. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial do fornecedor.

9.4.4.8. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9.4.4.9. Além disso, as licitantes devem apresentar:

a) juntamente com sua proposta comercial, documento detalhando as informações, local, site, páginas, documento, etc, necessários para aferição e atendimento de todos os itens da especificação técnica, ou seja, deverá apresentar uma espécie de índice ou planilha ponto-a-ponto, indicando o item, o documento que atende a especificação (com indicação do nome do documento), o local onde está disponibilizado o documento (URL, Site, ou outro disponibilizado de forma digital), a página e o texto que comprova o atendimento de cada item da especificação técnica.

b) ao menos uma das seguintes certificações ou outra equivalente: ICSA labs, NSS labs, Common Criteria.

c) por não inviabilizar o certame, pelo rol de fabricantes que possuem tais certificações, deverão apresentar

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

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

b) a declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

c) a comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

d) o registro previsto na Lei n. 5.764/1971, art. 107;

e) a comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

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

g) a última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de R$ 13.412.285,40 (treze milhões, quatrocentos e doze mil duzentos e oitenta e cinco reais e quarenta centavos), conforme custos unitários apostos na tabela do item 1.1 acima.

10.2. A estimativa de preços será precedida de regular pesquisa, nos moldes do art. 23 da Lei nº 14.133/21 e da Instrução Normativa SEGES/ME nº 65/2021, realizada pelo Setor de Compras e Contratações, na forma da referida Instrução Normativa, e dos valores recomendados pela Controladoria Geral do Cofen e aprovados pelo Plenário do Cofen.

10.3. Por se tratar de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

10.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea "d", inciso II do caput do art. 124 da Lei 14.133/2021.

10.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

10.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

10.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação

10.3.5. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado, por motivo superveniente, o Cofen convocará o fornecedor para negociar a redução do preço registrado e, caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

10.3.6. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao Cofen a alteração do preço registrado, mediante comprovação de fato superveniente que o impossibilite de cumprir o compromisso.

10.3.7. Em qualquer das hipóteses apresentadas, o Cofen convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam as condições.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Cofen no exercício de 2024 e serão alocados pelo Departamento Financeiro deste Conselho.

11.2. A contratação será atendida pela seguinte rubrica: 6.2.2.1.1.01.33.90.040 - Serviços Relacionados a Tecnologia da Informação.

12. DISPOSIÇÕES GERAIS

12.1. Os serviços especificados neste Termo de Referência não excluem outros, de natureza similar, que porventura se façam necessários para a boa execução da tarefa estabelecida pelo Contratante, obrigando-se a Contratada a executá-los prontamente como parte integrante de suas obrigações.

12.2. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

12.3. A apresentação de proposta implica na plena aceitação pela licitante adjudicatária das condições contidas neste Termo de Referência.

12.4. É proibida, por parte da Contratada, durante a vigência do contrato, a contratação de empregado pertencente ao quadro de colaboradores do Cofen.

12.5. A Contratada fica proibida de veicular publicidade acerca do objeto do Contrato, salvo se houver prévia e expressa autorização da Administração do Cofen.

13. ANEXOS DO TERMO DE REFERÊNCIA

13.1. Fazem parte e integram este Termo de Referência, para todos os fins e efeitos, os seguintes anexos:

13.1.1. ANEXO A - Endereços e Telefones;

13.1.2. ANEXO B - Especificações Técnicas;

13.1.3. ANEXO C - Prova Conceito;

13.1.4. ANEXO D - Níveis Mínimos de Serviços (NMS);

13.1.5. ANEXO E - Modelo de Declaração de Atendimento aos Critérios de Sustentabilidade Socioambiental;

13.1.6. ANEXO F - Modelo de Declaração de Vistoria

13.1.7. ANEXO G - Modelo de Termo de Compromisso e Manutenção de Sigilo e de Ciência de Manutenção de Sigilo;

13.1.8. ANEXO H - Modelo de Termo de Compartilhamento de Dados e Confidencialidade;

O presente documento segue assinado pelos Integrantes Requisitante e Técnico e pela autoridade responsável pela aprovação do Termo de Referência, com fulcro na Lei nº 14.133/2021 e no art. 30 da IN nº 05/2017-MPDG.

MATHEUS MOREIRA CRUZ
Integrante Técnico I

DAVI LUIZ ANDRADE LOPES VIEIRA
Integrante Requisitante/Autoridade Máxima da Área de TIC

Aprovado por:

LUIZ GUSTAVO PAULA DE MENEZES JUNIOR
Chefe do Departamento Técnico de Contratações
Portaria Cofen nº 744/2019

ANEXO A

1. **ENDEREÇOS E TELEFONES**

1.1. A sede do Cofen está atualmente localizada no seguinte endereço: SCLN QD 304, Lote 09, Bloco E, Asa Norte, Brasília/DF. A eventual alteração de endereço do Cofen, em razão da mudança para sua nova sede, localizada à EQS 208/209, Bloco A, Asa Sul, Brasília/DF, será comunicada oportunamente à Contratada para consequente alteração do local de realização das atividades contratadas, sem prejuízos, visto que a nova sede será próxima da atual, distando aproximadamente 8 km uma da outra. Telefone: (61) 3329-5871.

ANEXO B

ESPECIFICAÇÕES TÉCNICAS

1. **DESCRIÇÃO**

1.1. A tabela abaixo apresenta um resumo dos itens a serem contratados:

Item	Descrição do Serviço	CATSER	Desembolso	Métrica ou Unidade de Medida	Quantidade (a)
1	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	26999	mensal	unidade de serviço técnico	2

2	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	26999	mensal	unidade de serviço técnico	2
3	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	26999	mensal	unidade de serviço técnico	2
4	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	26972	único	unidade de serviço técnico	2
5	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	26972	único	unidade de serviço técnico	2
6	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	26972	único	unidade de serviço técnico	2
7	Serviços Técnicos Especializados	27332	sob demanda	horas/mês	50
8	Treinamento da Solução de Serviços Gerenciados de Firewall	3840	único	unidade	1
9	Serviços de Solução de proteção para Estações	26999	mensal	unidade de serviço técnico/mês	500
10	Serviços de Solução de proteção para Servidores	26999	mensal	unidade de serviço técnico/mês	200
11	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações	26999	mensal	unidade de serviço técnico/mês	500
12	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para servidores	26999	mensal	unidade de serviço técnico/mês	200

13	Instalação da solução de Segurança de Endpoints, Detecção e Respostas	26972	único	unidade de serviço técnico	500
14	Instalação da solução de Segurança de Servidores	26972	único	unidade de serviço técnico	200
15	Treinamento da Solução de Endpoints	3840	único	unidade	1
16	Serviços de Conectividade Local	26999	mensal	unidade de serviço técnico/mês	30
17	Instalação da solução de conectividade Local	26972	único	unidade de serviço técnico	30
18	Treinamento da Solução de Conectividade Local	3840	único	unidade	1
19	Serviços de Conectividade Wireless	26999	mensal	unidade de serviço técnico/mês	80
20	Instalação da solução de Conectividade Wireless	26972	único	unidade de serviço técnico	80
21	Treinamento da Solução e Conectividade Wireless	3840	único	unidade	1

2. ESPECIFICAÇÕES TÉCNICAS

2.1. São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos “possui”, “permite”, “suporta” e “é” implicam fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

2.2. Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada e estarem cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

2.3. Todos os equipamentos e softwares fornecidos para a prestação dos serviços deverão ser fornecidos com as Licenças durante toda a vigência do contrato.

2.4. O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança.

2.5. Ademais, todos os componentes necessários à prestação dos serviços, pertencentes ao mesmo lote, deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas e aos elencados do parque computacional do Contratante.

2.6. **ITENS 01, 02 e 03 – SERVIÇOS DE PROTEÇÃO DO TRÁFEGO DE REDE DE PRÓXIMA GERAÇÃO (ON PREMISE)** com as portas, conexões e cabeamentos disponibilizados pela Contratada, inclusive as SFP e SFP+ com as respectivas gbics)

2.6.1. CAPACIDADE E QUANTIDADES MÍNIMAS – Tipo A. A plataforma de segurança deve possuir no mínimo a capacidade e as características abaixo, por equipamento:

a) Performance mínima de 12 Gbps de throughput de IPS;

b) Performance mínima de 6.5 Gbps de throughput para Prevenção de Ameaças;

c) Performance mínima de 10 Gbps de throughput de NGFW;

d) Suporte a, no mínimo, 7.000.000 de conexões simultâneas;

e) Suporte a, no mínimo, 250.000 novas conexões por segundo;

f) Possuir o número irrestrito quanto ao máximo de usuários licenciados;

g) Possuir no mínimo 2 (duas) interfaces 10GbE SFP+ e 2 (duas) interfaces 1GE UTP;

h) Possuir 1 (uma) interface do tipo console ou similar;

i) Possuir 2 (duas) fonte 100-240VAC sendo pelo menos 1 opção hot-swap;

2.6.2. CAPACIDADE E QUANTIDADES MÍNIMAS – Tipo B. A plataforma de segurança deve possuir no mínimo a capacidade e as características abaixo, por equipamento:

a) Performance mínima de 5 Gbps de throughput de IPS;

b) Performance mínima de 3 Gbps de throughput para Prevenção de Ameaças;

c) Performance mínima de 3,5 Gbps de throughput de NGFW;

d) Suporte a, no mínimo, 3.000.000 de conexões simultâneas;

e) Suporte a, no mínimo, 100.000 novas conexões por segundo;

f) Possuir o número irrestrito quanto ao máximo de usuários licenciados;

g) Possuir no mínimo 2 (duas) interfaces 10GbE SFP+ e 2 (duas) interfaces 1GE UTP;

h) Possuir 1 (uma) interface do tipo console ou similar;

i) Possuir 2 (duas) fonte 100-240VAC sendo pelo menos 1 opção hot-swap;

2.6.3. CAPACIDADE E QUANTIDADES MÍNIMAS – Tipo C. A plataforma de segurança deve possuir no mínimo a capacidade e as características abaixo, por equipamento:

a) Performance mínima de 2.6 Gbps de throughput de IPS;

b) Performance mínima de 1 Gbps de throughput para Prevenção de Ameaças;

c) Performance mínima de 1,6 Gbps de throughput de NGFW;

d) Suporte a, no mínimo, 1.500.000 de conexões simultâneas;

e) Suporte a, no mínimo, 55.000 novas conexões por segundo;

f) Possuir o número irrestrito quanto ao máximo de usuários licenciados;

g) Possuir no mínimo 2 (duas) interfaces 1GbE SFP;

h) Possuir 1 (uma) interface do tipo console ou similar;

2.6.4. CARACTERÍSTICAS GERAIS PARA FIREWALL DE PRÓXIMA GERAÇÃO – Comuns aos Itens A, B e C:

2.6.4.1. Por terem a finalidade de proteger o ambiente tecnológico do Contratante que está exposto em toda rede mundial de computadores; por ser mais um item de averiguação técnica das soluções, certificando que passaram pelo crivo de organização especializada; e por não inviabilizar o certame, pelo rol de fabricantes que possuem tais certificações, deverão apresentar ao menos uma das seguintes certificações ou outra equivalente: ICSA labs, NSS labs, Common Criteria.

2.6.4.2. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e console de gerência, monitoração e logs.

2.6.4.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

2.6.4.4. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

2.6.4.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

2.6.4.6. O software deverá ser fornecido em sua versão mais atualizada.

2.6.4.7. Deve possuir modo HA (modo de alta disponibilidade) e deve ser implementado no mínimo ativo-passivo.

2.6.4.8. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

2.6.4.9. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

2.6.4.10. A atualização de software deverá enviar avisos de atualização automáticos.

2.6.4.11. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

2.6.4.12. O backup e o reestabelecimento de configuração deverão ser feito localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

2.6.4.13. As notificações deverão ser realizadas via email e SNMP.

2.6.4.14. Suportar SNMPv3 e Netflow.

2.6.4.15. O firewall deverá ser stateful, com inspeção profunda de pacotes.

2.6.4.16. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

2.6.4.17. As políticas de NAT deverão ser customizáveis para cada regra.

2.6.4.18. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

2.6.4.19. Proteção contra anti-spoofing.

2.6.4.20. Suportar IPv4 e IPv6.

2.6.4.21. O IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

2.6.4.22. Deve ter Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

2.6.4.23. Deve possuir tecnologia de conectividade SD-WAN.

2.6.4.24. Deve implementar balanceamento entre os links WAN com método SpillOver.

2.6.4.25. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN.

2.6.4.26. Deve suportar o uso de, no mínimo, 3 (três) links.

2.6.4.27. Deve suportar o uso de links de interfaces físicas, subinterfaces lógicas de VLAN e túneis IPSec.

2.6.4.28. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde.

2.6.4.29. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

2.6.4.30. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima.

2.6.4.31. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês.

2.6.4.32. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP para avaliação mais precisa de links que possuem QoE configurado.

2.6.4.33. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador.

2.6.4.34. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias.

2.6.4.35. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados.

2.6.4.36. Deve possibilitar o roteamento baseado em VPNs.

2.6.4.37. Deve suportar criar políticas de roteamento.

2.6.4.38. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

a) Interface de entrada do pacote;

b) IPs de origem;

c) IPs de destino;

d) Portas de destino;

e) Usuários ou grupos de usuários;

f) Aplicação em camada 7;

I - Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento.

II - Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

III - Deve suportar Extended VLAN.

IV - O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

V - A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces.

VI - Deve permitir a configuração de jumbo frames nas interfaces de rede.

VII - Deve permitir a criação de um grupo de portas layer2.

VIII - A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal.

IX - A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP; O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

X - A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

XI - Deve possuir otimização em tempo real de voz sobre IP.

XII - Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

2.6.5. CONTROLE POR POLÍTICAS DE FIREWALL

2.6.5.1. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

2.6.5.2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

2.6.5.3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

2.6.5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

2.6.5.5. Controle de políticas por países via localização por IP.

2.6.5.6. Suporte a objetos e regras IPV6.

2.6.5.7. Suporte a objetos e regras *multicast.*

2.6.6. PREVENÇÃO DE AMEAÇAS

2.6.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

2.6.6.2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

2.6.6.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

2.6.6.4. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras.

2.6.6.5. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa.

2.6.6.6. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem.

2.6.6.7. Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning.

2.6.6.8. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware e, ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma.

2.6.6.9. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem.

2.6.6.10. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

2.6.6.11. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

2.6.6.12. Deve ter proteção em tempo real contra novas ameaças criadas.

2.6.6.13. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

2.6.6.14. Deve permitir o bloqueio de vulnerabilidades.

2.6.6.15. Deve permitir o bloqueio de exploits conhecidos.

2.6.6.16. Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

2.6.6.17. Deve incluir proteção contra ataques de negação de serviços.

2.6.6.18. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

2.6.6.19. Suportar bloqueio de arquivos por tipo.

2.6.6.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

2.6.6.21. Os eventos devem identificar o país de onde partiu a ameaça.

2.6.6.22. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança. O apliance deve ter a capacidade de atuar como um gateway antispam de modo que possa realizar filtragens dos emails e aplicar políticas.

2.6.6.23. O gateway de email incluso no apliance deve ter pelo menos as seguintes proteções:

a) Sender Policy Framework (SPF);

b) Domain Keys Identified Mail (DKIM);

c) Domain-based Message Authentication, Reporting & Conformance (DMARC);

d) Bounce Address Tag Validation (BATV).

2.6.6.24. O filtro de email deve quarentenar os emails suspeitos ou realmente maliciosos.

2.6.6.25. A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens.

2.6.6.26. A função de antispam deve permitir a configuração de relays com a possibilidade de autenticação desses relays. A função de antispam deve possibilitar também o envio de emails seguros, realizando a criptografia das mensagens bem como dos seus anexos.

2.6.6.27. A função de antispam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas.

2.6.6.28. O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevenção dos ataques de path traversal ou directory traversal.

2.6.6.29. O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

2.6.6.30. O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de ranges de IP.

2.6.6.31. Deverá permitir a identificação dos IPs de origem através de proxy via “X-forward headers”.

2.6.6.32. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

2.6.6.33. Proteção pelo menos contra os seguintes ataques, mas não limitada a: SQL injection e Cross-site scripting.

2.6.7. CONTROLE E PROTEÇÃO DE APLICAÇÕES

2.6.7.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

2.6.7.2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos TLS 1.2 e TLS 1.3.

2.6.7.3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

2.6.7.4. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

2.6.7.5. Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

2.6.7.6. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP, Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

2.6.7.7. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive, File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).

2.6.7.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.6.7.9. Atualizar a base de assinaturas de aplicações automaticamente.

2.6.7.10. Reconhecer aplicações em IPv6.

2.6.7.11. Limitar a banda usada por aplicações (*traffic shaping*).

2.6.7.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.

2.6.7.13. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

2.6.7.14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

2.6.8. CONTROLE E PROTEÇÃO WEB

2.6.8.1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

2.6.8.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

2.6.8.3. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Azure AD, Radius, *E-directory* e base de dados local.

2.6.8.4. Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius.

2.6.8.5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

2.6.8.6. Possuir pelo menos 90 categorias de URLs.

2.6.8.7. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.6.8.8. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca.

2.6.8.9. Deve ser capaz de forçar as restrições do Youtube.

2.6.8.10. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário.

2.6.8.11. Suportar a criação categorias de URLs customizadas.

2.6.8.12. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

2.6.8.13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada.

2.6.8.14. Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

2.6.8.15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

2.6.8.16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem.

2.6.8.17. Deve realizar caching do conteúdo web.

2.6.8.18. Deve realizar filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

2.6.8.19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

2.6.8.20. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

2.6.8.21. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

2.6.8.22. A solução deve permitir o enforce dos domínios do Google e Office365 afim de determinar em quais domínios os usuários poderão se autenticar.

2.6.9. IDENTIFICAÇÃO DE USUÁRIOS

2.6.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Azure AD, Radius, eDirectory, TACACS+* e via base de dados local para identificação de usuários e grupos, permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

2.6.9.2. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

2.6.9.3. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

2.6.9.4. Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multissessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

2.6.9.5. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory.

2.6.9.6. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

2.6.10. QUALIDADE DE SERVIÇO - QoS

2.6.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

2.6.10.2. A solução deverá suportar *Traffic Shaping* (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

2.6.10.3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.

2.6.10.4. Suportar priorização *Real-Time* de protocolos de voz (VoIP).

2.6.10.5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

2.6.11. REDES VIRTUAIS PRIVADAS - VPN

2.6.11.1. Suportar VPN *Site-to-Site e Cliente-to-Site*.

2.6.11.2. Suportar IPsec VPN.

2.6.11.3. Suportar SSL VPN.

2.6.11.4. Suportar L2TP e PPTP.

2.6.11.5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

2.6.11.6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

2.6.11.7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows e macOS.

2.6.11.8. Deve possuir opção de VPN IPSEC com client nativo do fabricante.

2.6.11.9. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

2.6.11.10. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

2.6.11.11. Deve suportar nativamente a integração com a huawei, afim de estabelecer um túnel seguro entre os appliances e o VPN da huawei.

2.6.11.12. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

2.6.11.13. Suportar autenticação via AD/LDAP, *Token* e base de usuários local.

2.6.11.14. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, *Active Directory, Azure AD, Radius, eDirectory, TACACS+* e via base de dados local.

2.6.12. GERÊNCIA ADMINISTRATIVA CENTRALIZADA

2.6.12.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

2.6.12.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

2.6.12.3. Estar licenciada para ser gerenciada pela console de gerenciamento do firewall.

2.6.12.4. Devem ser fornecidas soluções virtuais ou em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação.

2.6.12.5. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para estas soluções de firewall, sem necessidade de acesso direto aos equipamentos.

2.6.12.6. Deve permitir a criação de templates para configurações.

2.6.12.7. Deve possuir indicadores do estado de equipamentos e rede.

2.6.12.8. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

2.6.12.9. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

2.6.12.10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc).

2.6.12.11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas.

2.6.12.12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

2.6.12.13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

2.6.12.14. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

2.6.13. GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

2.6.13.1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

2.6.13.2. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo A.

2.6.13.3. Devem ser fornecidas soluções virtuais ou em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 8TB de dados.

2.6.13.4. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando. Deve possibilitar a identificação de ataques como a detecção de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

2.6.13.5. Deve conter relatórios pré-configurados pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN.

2.6.13.6. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

2.6.13.7. Deve conter customizações dos relatórios para inserção de logotipos próprios.

2.6.13.8. Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

2.6.13.9. Deve permitir a exportação via PDF ou Excel.

2.6.13.10. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

2.6.13.11. Deve fornecer relatórios de tendências.

2.6.13.12. Deve fornecer logs em tempo real, de auditoria e arquivados.

2.6.13.13. Deve possuir mecanismo de procura de logs arquivados.

2.6.13.14. Deve ter acesso baseado em Web com controles administrativos distintos.

2.6.14. A Contratada deverá fornecer tudo que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

2.7. **ITENS 04, 05, 06 – IMPLANTAÇÃO DAS SOLUÇÕES INTEGRADAS DE SEGURANÇA**

2.7.1. A Contratada deverá oferecer implantação das soluções, com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato e de acordo com as regras e políticas exigidas pela equipe técnica do Contratante, dentro do escopo das funcionalidades de cada serviço definidas neste Termo.

2.7.2. Deverão ser apresentados os seguintes entregáveis durante a implantação:

2.7.2.1. Fase de desenho da arquitetura.

2.7.2.2. Esquema detalhado de conexão com dispositivos.

2.7.2.3. Fase de Instalação.

2.7.3. A Contratada confeccionará relatório(s) final(is) sobre as atividades realizadas e com recomendações ao Contratante. Este relatório poderá ser entregue em até 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

2.7.3.1. Introdução;

2.7.3.2. Análise do ambiente;

2.7.3.3. Atividades realizadas;

2.7.3.4. Configuração de políticas aplicadas;

2.7.3.5. Resultados obtidos (coberturas, eventos de segurança registrados);

2.7.3.6. Conclusões;

2.7.3.7. Recomendações Específicas;

2.7.3.8. Recomendações de Segurança Corporativa;

2.7.4. Todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos do Contratante.

2.7.5. A implantação das soluções, quando realizada no ambiente de produção, poderá ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados).

2.7.6. A Contratada será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do Contratante, sem prejuízo aos serviços desta.

2.7.7. Quando previamente acordado entre as partes, a Contratada poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante da instituição.

2.7.8. A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executada pela Contratada nos prédios do Contratante.

2.7.9. Deve abranger a instalação física e lógica da solução, em sua totalidade, com duração máxima de 7 (sete) dias corridos, compreendendo, mas não se limitando a essas, as seguintes atividades:

2.7.9.1. Instalação física ou virtual dos equipamentos nas dependências ou no ambiente tecnológico do Contratante.

2.7.9.2. Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sentido de melhorar o gerenciamento e performance e aplicar os "*patchs*" para atualização do sistema, quando necessário.

2.7.9.3. Definição das funcionalidades a serem implantadas.

2.7.9.4. Definição da parametrização.

2.7.9.5. Instalação e configuração de toda a solução com vista ao gerenciamento dos recursos solicitados neste Termo em sua totalidade.

2.7.10. A instalação deve contemplar a verificação da infraestrutura elétrica e lógica existente. Eventuais problemas e necessidade de ajustes devem ser comunicados ao Contratante o qual será responsável pela solução de tais problemas.

2.7.11. A instalação dos equipamentos e componentes da solução deverá levar em consideração o ambiente e instalações existentes (espaço físico, sistema de refrigeração e de fornecimento de energia elétrica, dutos, eletrocalhas, entre outros elementos). Os componentes fornecidos (equipamentos e acessórios) devem proporcionar condições ideais de funcionamento tanto no que diz respeito à disposição física nas salas e nos "rack's" evitando problemas de refrigeração e de acesso físico.

2.7.12. Após a instalação dos equipamentos, alimentação elétrica e conexões com a rede de dados e/ou voz, não poderá haver cabos sem proteção, soltos, por cima do piso elevado ou que obstruam a frente ou visibilidade dos equipamentos instalados.

2.7.13. Os serviços de instalação e configuração deverão ser prestados nas dependências do Contratante.

2.7.14. REQUISITOS GERAIS PARA A PRESTAÇÃO DOS SERVIÇOS

2.7.14.1. É responsabilidade da Contratada quaisquer danos físicos aos equipamentos durante os processos de instalação e configuração.

2.7.14.2. É proibida a divulgação de quaisquer aspectos da configuração desses equipamentos, por questões de sigilo e segurança, por parte dos técnicos responsáveis pela instalação e configuração, ou quaisquer outros que tenham acesso a essas informações, salvo quando houver autorização por escrito do Contratante.

2.7.14.3. Todas as senhas criadas e os usuários cadastrados nos processos de instalação e configuração dos equipamentos devem ser registrados e entregues por escrito ao responsável técnico indicado pelo Cofen.

2.7.14.4. Deverá ser entregue ao responsável técnico indicado pelo Cofen relatório com todos os procedimentos e configurações executados, assinado pelo responsável técnico da Contratada.

2.7.14.5. O início dos serviços deve ocorrer obedecendo os prazos dispostos neste termo.

2.7.14.6. A Contratada deve executar, prioritariamente, como parte obrigatória do processo de instalação e sempre que aplicável a cada solução, as seguintes atividades:

a) Definição de políticas e regras de proteção do perímetro "*internet*" visando conformidade com as normas ISO/IEC 17799 e NBR-ISO/IEC 17799, que tratam de segurança da informação e das configurações abaixo;

b) Configuração da console de gerenciamento;

c) Migração das regras existentes na solução de segurança atual do Contratante;

d) Configuração da autenticação de usuários integrada ao domínio da rede "*Microsoft*", via ferramenta nativa de integração da solução;

e) Análise de falsos positivos que podem ser gerados após implantação;

f) Adequações pós-instalação;

g) Instalação e configuração dos "*firewall's*" em modo "*cluster*" ativo/ativo ou ativo/passivo;

h) Instalação e configuração do concentrador de "*logs*", "*archive*" e relatórios;

i) Instalação e configuração dos "*gateway's*" "*SMTP*" em modo "*cluster*" ativo/ativo ou ativo/passivo;

j) Migração, adequação e definição, juntamente com a equipe de Tecnologia da Informação do Contratante das políticas para controle de tráfego de entrada e saída de dados;

k) Execução de testes de segurança através da análise de vulnerabilidades completa do perímetro de internet;

l) Documentação de todas as configurações realizadas em todas as soluções implantadas;

m) Realização de testes, certificação e otimização de todas as soluções implantadas;

n) Entrega da documentação de todo o projeto.

2.8. ITEM 07 – SERVIÇOS TÉCNICOS ESPECIALIZADOS

2.8.1. A Contratada deverá disponibilizar, sob demanda, horas de serviços técnicos especializados em segurança da informação, de forma a atender aos seguintes requisitos:

2.8.1.1. É prevista a utilização média de 600 (seiscentas) horas por ano.

2.8.1.2. Não há garantia de execução das 600 horas, tratando-se apenas de previsão estimativa.

2.8.1.3. Os serviços elegíveis a serem executados limitar-se-ão, exclusivamente, aos seguintes casos:

I - elaboração de pareceres em segurança da informação.

II - análise de segurança em elementos que não sejam de propriedade da Contratada ou que não estejam no escopo desse projeto.

III - suporte aos planos de melhoria na infraestrutura de segurança do Contratante.

IV - suporte a mudanças de arquitetura do ambiente do Contratante, sobretudo aos aspectos de segurança envolvidos.

V - avaliação de vulnerabilidades da rede do Contratante, fora do escopo desse projeto, incluindo a indicação de atualizações ou procedimento necessários para mitigá-las.

VI - apoio na definição e implementação de mecanismos futuros de monitoramento de segurança.

VII - configuração de segurança e atualização de versão de softwares de equipamentos de rede, excluídos os equipamentos de propriedade da Contratada.

VIII - orientação quanto a procedimentos de auditoria forense no ambiente computacional do Contratante.

IX - elaboração, em conjunto com o Contratante, de planos de conscientização de usuários que proporcionem maior grau de segurança.

X - mudanças de endereço: incluem-se no escopo dos serviços a desinstalação, o transporte para o novo endereço e a reinstalação de todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços.

XI - transferência de conhecimento às pessoas indicadas pelo Contratante (até seis pessoas por evento), por meio de workshops, conforme as características abaixo:

a) ser realizado nas dependências do Contratante;

b) ter duração máxima de 8 (oito) horas;

c) ter como conteúdo os conhecimentos referentes a operação, administração, procedimentos e incidentes ocorridos e respectivas ações de mitigação, problemas vivenciados e soluções aplicadas e mudanças de arquitetura ou de tecnologia, além de informações necessárias à transição contratual.

2.8.1.4. Não serão passíveis de execução por meio de utilização dos Serviços Técnicos Especializados as atividades elencadas nos demais itens e tópicos deste anexo.

2.8.1.5. Para a execução dos serviços especificados neste item, a Contratada deverá alocar pelo menos um profissional que detenha comprovação de conhecimento técnico no produto ou serviços a serem prestados, a ser

comprovada no momento do recebimento da ordem de serviço.

2.8.1.6. Condições de execução dos serviços:

I - os serviços serão executados nas instalações do Contratante, por técnicos da empresa Contratada detentores do perfil adequado.

II - quaisquer serviços ou procedimentos realizados deverão ser previamente aprovados pelo Contratante por meio de Ordem de Serviço, disposto neste Termo, em comum acordo entre o Contratante e a Contratada, sendo que o tempo necessário ao atendimento deverá ser previamente definido na respectiva Ordem de Serviço.

III - a prorrogação do prazo de execução de uma Ordem de Serviço somente será possível mediante apresentação, pela Contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pelo Contratante, ou por interesse do Contratante, em caso de impedimento devidamente justificado que dificulte ou não permita a execução dos serviços.

IV - as ordens de serviço só serão consideradas concluídas após a entrega da documentação dos procedimentos e da configuração resultante nas bases e nos padrões definidos pelo Contratante (incluindo documento as-built).

V - para recebimento dos serviços será preenchido o Termo de Recebimento de Serviços.

VI - o Contratante deve avaliar os produtos entregues em até 10 (dez) dias contados da entrega dos serviços/produtos exigidos.

VII - a Contratada deverá reapresentar os serviços/itens corrigindo eventuais observações feitas pelo Contratante em até 10 (dez) dias, a contar da comunicação pelo Contratante.

VIII - caso o Contratante avalie o material corrigido como insuficiente ou inadequado, a Contratada será considerada em atraso até que sejam sanadas todas as pendências.

IX - estando todos os elementos necessários, o Contratante fará o recebimento definitivo dos serviços no prazo em até 10 (dez) dias contados do recebimento provisório.

X - o Contratante somente autorizará o pagamento das faturas emitidas após o recebimento definitivo, realizado mensalmente, de acordo com os níveis mínimos de serviço estabelecidos.

2.9. **ITENS 09, 10, 11 e 12, 13 e 14 – SERVIÇOS E INSTALAÇÃO DE SEGURANÇA DE ESTAÇÕES E SERVIDORES:**

2.9.1. CARACTERÍSTICAS GERAIS:

2.9.1.1. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional.

2.9.1.2. Deve possuir mecanismo de comunicação via API para integração com outras soluções de segurança, como por exemplo SIEM.

2.9.1.3. Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores.

2.9.1.4. A console deve permitir a divisão dos computadores dentro da estrutura de gerenciamento em grupos.

2.9.1.5. Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

2.9.1.6. Deve possuir a possibilidade de aplicar regras diferenciadas baseada em grupos ou usuários.

2.9.1.7. A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas.

2.9.1.8. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando.

2.9.1.9. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos.

2.9.1.10. Deve permitir exclusões de escaneamento para determinados websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

2.9.1.11. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs.

2.9.1.12. Atualização incremental, remota e em tempo real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes.

2.9.1.13. Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador.

2.9.1.14. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador.

2.9.1.15. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

2.9.1.16. As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

2.9.1.17. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF.

2.9.1.18. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.

2.9.1.19. Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status.

2.9.1.20. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

a) Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhamento desses usuários;

b) Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

c) Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

d) Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

e) Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

f) Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

g) Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados;

2.9.1.21. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada.

2.9.1.22. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais.

2.9.1.23. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo.

2.9.1.24. As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

2.9.1.25. A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

2.9.1.26. O agente anti-vírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web.

2.9.1.27. Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá

ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos.

2.9.1.28. Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente.

2.9.1.29. Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;

2.9.1.30. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo.

2.9.1.31. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio.

2.9.1.32. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais.

2.9.1.33. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoints e servidores.

2.9.1.34. Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro).

2.9.1.35. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança.

2.9.1.36. Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção.

2.9.1.37. Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc) e classificar os PCs em conformidade.

2.9.1.38. Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

a) Proteger o dispositivo com a opção de início de uma varredura;

b) Forçar uma atualização naquele momento;

c) Ver os detalhes dos eventos ocorridos;

d) Executar verificação completa do sistema;

e) Forçar o cumprimento de uma nova política de segurança;

f) Mover o computador para outro grupo;

g) Apagar o computador da lista;

h) Atualizar políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

2.9.1.39. Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses.

2.9.1.40. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF.

2.9.1.41. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints.

2.9.1.42. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

a) Nome do dispositivo;

b) Início da proteção;

c) Último usuário logado no dispositivo;

d) Último update;

e) Último escaneamento realizado;

f) Status de proteção do dispositivo;

g) Grupo a qual o dispositivo faz parte;

h) Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;

2.9.1.43. A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente.

2.9.2. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

2.9.2.1. Características básicas do agente de proteção contra malwares:

I - A solução deverá ser capaz de proteger estações de trabalho contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nas estações de trabalho.

II - Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos.

III - O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos.

IV - O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças.

V - O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes.

VI - A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

VII - Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot.

VIII - Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados.

IX - Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA).

X - Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados.

XI - Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos.

XII - É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs).

XIII - Suportar máquinas com arquitetura 32-bit e 64-bit.

XIV - O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais macOS 12, 13 e 14 e Microsoft Windows 10 e 11.

XV - Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações.

XVI - Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

XVII - Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

2.9.2.2. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

I - Possuir proteção contra exploração de buffer overflow.

II - Deverá possuir atualização periódica de novas assinaturas de ataque.

III - Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

IV - Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas.

V - Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

VI - Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

VII - Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

d) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

e) Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.9.2.3. Funcionalidade de Antivírus e AntiSpyware:

I - Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

II - Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

III - As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus.

IV - Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto.

V - Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário.

VI - Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus.

VII - Capacidade de detectar arquivos através de sua reputação.

VIII - Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

IX - A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante.

X - Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede.

XI - Deverá detectar tráfego de rede para comandar e controlar as estações de trabalho.

XII - Proteger arquivos de documento contra ataques do tipo ransomwares.

XIII - Proteger que o ataque de ransomware seja executado remotamente.

XIV - Permitir o bloqueio da verificação de vírus em recursos mapeados da rede.

XV - Antivírus de Web (verificação de sites e downloads contra vírus).

XVI - Controle de acesso a sites por categoria.

XVII - Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

XVIII - O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista de sites sempre permitidos e lista de sites que devem ser bloqueados sempre.

XIX - Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio.

XX - Capacidade de verificar somente arquivos novos e alterados.

XXI - Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante.

XXII - Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças.

XXIII - Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas.

XXIV - Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.9.2.4. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

I - Funcionalidade de detecção de ameaças via técnicas de machine learning.

II - Funcionalidade de detecção de ameaças desconhecidas que estão em memória.

III - Capacidade de detecção e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística).

IV - Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória.

V - Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.9.2.5. Funcionalidade de proteção contra ransomwares:

I - Dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

II - Dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

III - Dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação

IV - A solução deverá previnir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

V - Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

VI - Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

a) DEP (Data Execution Prevention);

b) Address Space Layout Randomization (ASLR);

c) Bottom Up ASLR;

d) Null Page;

e) Anti-HeapSpraying;

f) Dynamic Heap Spray;

g) Import Address Table Filtering (IAF);

h) VTable Hijacking;

i) Stack Pivot and Stack Exec;

j) SEHOP;

k) Stack-based ROP (Return-Oriented Programming);

l) Control-Flow Integrity (CFI);

m) Syscall;

n) WOW64;

o) Load Library;

p) Shellcode;

q) VBScript God Mode;

r) Application Lockdown;

s) Process Protection;

t) Network Lockdown.

VII - A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

VIII - Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

IX - A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentes para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

X - A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.9.2.6. Funcionalidade de Controle de aplicações e dispositivos:

I - Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede.

II - Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada.

III - Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web.

IV - Oferecer proteção para chaves de registro e controle de processos.

V - Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo.

VI - Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar.

VII - Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo.

VIII - Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos.

IX - Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo.

X - As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

XI - Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

XII - A gestão desses dispositivos deverá feita diretamente no console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints.

XIII - Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

a) Permitir todos os dispositivos do mesmo modelo;

b) Permitir um único dispositivo com base em seu número de identificação único;

c) Permitir o acesso total;

d) Permitir acesso somente leitura;

e) Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.9.2.7. Funcionalidade de Proteção e Prevenção a Perda de Dados:

I - Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo.

II - Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo).

III - Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se realmente quer transferir o arquivo identificado como sensível.

IV - Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

a) Números de cartões de crédito;

b) Números de contas bancárias;

c) Números de Passaportes;

d) Endereços;

e) Números de telefone;

f) Códigos postais definidos por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

g) Lista de e-mails;

h) Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

V - Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade.

VI - Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

VII - Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e, em todos os casos, gravar a operação realizada com as principais informações da operação.

VIII - Permitir o controle de dados para, no mínimo, os seguintes meios:

a) Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

b) Anexado no navegador (ao menos IE, Firefox e Chrome);

c) Anexado no cliente de mensagens instantâneas (ao menos Skype);

d) Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

2.9.2.8. Funcionalidade de Endpoint Detection and Response (EDR):

I - A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas.

II - Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a

nuvem de inteligência do fabricante.

III - Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

IV - Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

a) Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

b) Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

c) Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

d) Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado. A solução de EDR deverá ser integrada ao agente de antivírus a ser instalada com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

V - O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus.

VI - Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder.

VII - Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça.

VIII - Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando.

IX - Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado.

X - Deve possibilizar o agendamento de consultas (queries).

XI - Deve reter os dados no Data Lake por no mínimo 7 dias.

2.9.2.9. Funcionalidade de Extended Detection And Response (XDR):

I - Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado.

II - Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL ou similar.

III - Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito.

IV - Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos.

V - Deve disponibilizar pontos de aplicação que permitem executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware.

VI - Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização.

VII - Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas.

VIII - Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes.

IX - Deve reter os dados no Data Lake por no mínimo 30 dias.

X - O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud.

XI - A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar

evidências de ataques ou eventos suspeitos existentes dentro do ambiente.

XII - Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento.

XIII - Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console.

XIV - Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console.

XV - A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação.

XVI - Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação.

2.9.3. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

2.9.3.1. Características básicas do agente de proteção contra malwares:

I - A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores.

II - Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos.

III - O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos.

IV - O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes.

V - A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

VI - Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot.

VII - Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados.

VIII - Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA).

IX - Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados.

X - Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos.

XI - É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs).

XII - Suportar máquinas com arquitetura 32-bit e 64-bit.

XIII - O cliente para instalação em servidores deverá ser compatível com os sistemas operacionais abaixo:

a) Windows Server 2012;

b) Windows Server 2016;

c) Windows Server 2019;

d) Windows Server 2022;

e) Debian 10/11/12;

f) CentOS 7/8;

g) Oracle Linux 8/9;

h) Red Hat Enterprise Linux 7/8;

i) SUSE 12/15;

j) Ubuntu Server 20.04/22.04;

XIV - Deve possuir integração com as nuvens da Microsoft Azure, Amazon Web Services, Google Cloud e Huawei Cloud para identificar as informações dos servidores instanciados nas nuvens.

XV - Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

XVI - Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

XVII - Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers e afins.

XVIII - A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

a) Escalação de privilégios dentro de containers;

b) Programas utilizando técnicas de mineração de criptomoedas;

c) Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

d) Detecção de funções internas do kernel que estão sendo adulteradas em um host;

XIX - A solução deve também se integrar a tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas.

2.9.3.2. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

I - Possuir proteção contra exploração de buffer overflow.

II - Deverá possui atualização periódica de novas assinaturas de ataque.

III - Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

IV - Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas.

V - Possuir um sistema de prevenção de intrusão no host (HIPS) que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

VI - Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução para detectar comportamento suspeito de aplicações, tais como buffer overflow.

VII - Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

d) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo .jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

e) Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

2.9.3.3. Funcionalidade de Antivírus e AntiSpyware:

I - Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

II - Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

III - As configurações do antispyware deverão ser realizadas através da mesma console do antivírus.

IV - Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto.

V - Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores.

VI - Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus.

VII - Capacidade de detectar arquivos através de sua reputação.

VIII - Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

IX - A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante.

X - Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede.

XI - Deverá detectar tráfego de rede para comandar e controlar os servidores.

XII - Proteger arquivos de documento contra ataques do tipo ransomwares.

XIII - Proteger que o ataque de ransomware seja executado remotamente.

XIV - Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante.

XV - Permitir o bloqueio da verificação de vírus em recursos mapeados da rede.

XVI - Antivírus de Web (verificação de sites e downloads contra vírus).

XVII - Controle de acesso a sites por categoria.

XVIII - Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

XIX - O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista de sites sempre permitidos e de lista de sites que devem ser bloqueados sempre.

XX - Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio.

XXI - Capacidade de verificar somente arquivos novos e alterados.

XXII - Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

XXIII - Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças.

XXIV - Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas.

2.9.3.4. Funcionalidade de detecção Pró-ativa de reconhecimento de novas ameaças:

I - Funcionalidade de detecção de ameaças via técnicas de machine learning.

II - Funcionalidade de detecção de ameaças desconhecidas que estão em memória.

III - Capacidade de detecção e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos

(ataques de dia zero) através da análise de comportamento de processos em memória (heurística).

IV - Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória.

V - Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.9.3.5. Funcionalidade de proteção contra ransomwares:

I - Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas.

II - Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares.

III - Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.

IV - A solução deverá previnir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

V - Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

VI - Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

a) DEP (Data Execution Prevention);

b) Address Space Layout Randomization (ASLR);

c) Bottom Up ASLR;

d) Null Page;

e) Anti-HeapSpraying;

f) Dynamic Heap Spray;

g) Import Address Table Filtering (IAF);

h) VTable Hijacking;

i) Stack Pivot and Stack Exec;

j) SEHOP;

k) Stack-based ROP (Return-Oriented Programming);

l) Control-Flow Integrity (CFI);

m) Syscall;

n) WOW64;

o) Load Library;

p) Shellcode;

q) VBScript God Mode;

r) Application Lockdown;

s) Process Protection;

t) Network Lockdown.

VII - A solução deverá trabalhar silenciosamente no servidor e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware no servidor.

VIII - Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

IX - A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

X - A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.9.3.6. Funcionalidade de Controle de aplicações e dispositivos:

I - Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede.

II - Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada.

III - Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web.

IV - Oferecer proteção para chaves de registro e controle de processos.

V - Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo.

VI - Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar.

VII - Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo.

VIII - Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos.

IX - Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo.

X - As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

XI - Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

XII - A gestão desses dispositivos deverá feita diretamente no console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints.

XIII - Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

a) Permitir todos os dispositivos do mesmo modelo;

b) Permitir um único dispositivo com base em seu número de identificação único;

c) Permitir o acesso total;

d) Permitir acesso somente leitura;

e) Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.9.3.7. Funcionalidade de Proteção e Prevenção a Perda de Dados:

I - Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo.

II - Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo).

III - Possibilitar o bloqueio, somente registrar o evento na console de administração, ou perguntar ao usuário se realmente quer transferir o arquivo identificado como sensível.

IV - Deve possuir listas de CCLs pré-configuradas com, no mínimo, as seguintes identificações:

a) Números de cartões de crédito;

b) Números de contas bancárias;

c) Números de Passaportes;

d) Endereços;

e) Números de telefone;

f) Códigos postais definidos por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

g) Lista de e-mails;

h) Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

V - Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade.

VI - Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

VII - Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e, em todos os casos, gravar a operação realizada com as principais informações da operação.

VIII - Permitir o controle de dados para no mínimo os seguintes meios:

a) Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

b) Anexado no navegador (ao menos IE, Firefox e Chrome);

c) Anexado no cliente de mensagens instantâneas (ao menos Skype);

d) Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

2.9.3.8. Funcionalidade de Endpoint Detection and Response (EDR)

I - A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas.

II - Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

III - Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

IV - Após a análise da nuvem de inteligência do fabricante, a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

a) Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

b) Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

c) Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

d) Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final.

V - O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus.

VI - Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado e como responder.

VII - Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça.

VIII - Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando.

IX - Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado.

X - Deve possibilitar o agendamento de consultas (queries).

XI - Deve reter os dados no Data Lake por no mínimo 7 dias.

2.9.3.9. Funcionalidade de Extended Detection And Response (XDR) - a Contratada deverá fornecer tudo que for necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente:

I - Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado.

II - Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL ou similar.

III - Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito.

IV - Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos.

V - Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware.

VI - Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização.

VII - Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas.

VIII - Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes.

IX - Deve reter os dados no Data Lake por no mínimo 30 dias.

X - O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud Microsoft Azure, Amazon Web Services, Google Cloud, Huawei Cloud, Tencent Cloud e Oracle Cloud.

XI - A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente.

XII - Tais detecções e evidências devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento.

XIII - Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console.

XIV - Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual diversos eventos e detecções encontradas na console.

XV - A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação.

XVI - Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação.

2.9.3.10. Serviços de detecção e resposta 24/7, suportado pela fabricante da solução de proteção para estações e servidores

I - A Contratada deverá prover serviço de busca, detecção e resposta a ameaças avançadas do fabricante da solução de segurança ofertada.

II - Este serviço deve ter funcionamento 24x7 e deve contar com time de especialistas do fabricante das soluções de proteção de estações e servidores ofertada.

III - Deve disponibilizar (licitante e/ou fabricante) equipes especializadas em, no mínimo, 2 SOCs separados geograficamente, a fim de manter redundância do serviço.

IV - Deve prover relatórios com resumos das atividades e incidentes de segurança encontrados no ambiente do Contratante.

V - Deve prover a verificação da integridade dos componentes da solução de segurança instalada no ambiente do Contratante.

VI - A solução de MDR deve ser gerenciada na mesma plataforma da solução XDR ou homologada pelos fabricantes distintos demonstrando explicitamente que todas funcionalidades estão disponibilizadas na integração.

VII - A plataforma deverá coletar dados de segurança e telemetria de várias fontes de produtos instalados no ambiente do Contratante.

VIII - Deverá trabalhar com ferramentas de segurança e serviços de MDR de maneira integrada.

IX - Deve operar sem a necessidade de substituir as ferramentas de segurança existentes.

X - O serviço poderá ser fornecido usando ferramentas integradas do fabricante, ferramentas de terceiros ou a combinação dos dois.

XI - Deve proporcionar níveis de serviço personalizados, desde notificação detalhada até resposta a incidentes em grande escala.

XII - Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do fabricante ou homologada pelos fabricantes distintos demonstrando explicitamente que todas funcionalidades estão disponibilizadas na integração.

XIII - Deve ser compatível com integrações de terceiros, contendo as seguintes categorias e, no mínimo, os fabricantes a seguir:

a) Firewalls:

- Check Point;
- Palo Alto;
- Fortinet;
- Cisco;
- SonicWall;
- Sophos;
- Watchguard.

b) Endpoints:

- Microsoft;
- CrowdStike;
- McAfee;
- SentinelOne;
- Check Point;
- Trend Micro;
- Malwarebytes;
- BalckBerry;
- Palo Alto Cortex XDR;
- Sophos.

c) Provedores de identidade:

- Microsoft Azure IDP, ATA;
- Okta;
- Duo.

d) Plataformas de filtragem de e-mails:

- Microsoft 365;

- Mimecast;
- Proofpoint.

e) Infraestrutura de nuvens públicas:

- Amazon Web Services;
- Microsoft Azure;
- Google Cloud;
- Huawei Cloud;
- Tencent Cloud;
- Orca Security;
- Prisma Cloud;
- Oracle Cloud.

f) Monitoramento de Redes:

- Darktrace;
- Hillstone;
- Forcepoint.

XIV - As integrações de terceiros poderão ser via API ou envio de Syslogs.

XV - A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema para uso em nuvem.

XVI - O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados para eventuais consultas.

XVII - O serviço de busca, detecção e resposta a ameaças avançadas deverá prover ao Contratante:

a) Notificações sobre detecções e detalhes das ameaças encontradas no ambiente;

b) Mitigação de incidentes relacionados a ameaças nos dispositivos cobertos com a solução fazendo a contenção de ameaças: os ataques devem ser interrompidos, evitando a propagação;

c) Análise de causa raiz realizada para evitar recorrências futuras;

d) Canais de comunicação com os especialistas do fabricante para sanar dúvidas, dar respostas à incidentes e autorizar mudanças e ações preventivas no ambiente computacional do Contratante.

2.9.4. CARACTERÍSTICAS GERAIS DO SERVIÇO DE INSTALAÇÃO

2.9.4.1. É/será de inteira responsabilidade da Contratada a correta instalação, configuração e funcionamento dos endpoints e componentes da solução ofertada. Os endpoints e componentes serão implementados pela Contratada de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento dos endpoints ou componentes fora das condições normais recomendadas pelo fabricante.

2.9.4.2. A instalação e configuração deve ser implementada On-Line conforme cenário fornecido pelo DTIC/Cofen após assinatura do contrato.

2.9.4.3. A empresa Contratada deverá realizar toda a instalação da solução adquirida e quaisquer outras providências que tenham relação direta com a instalação do serviço em questão.

2.9.4.4. Usuários do DTIC/Cofen deverão possuir privilégios de administradores.

2.9.4.5. Após o recebimento da ordem de serviço (OS), a Contratada deverá apresentar, no prazo máximo de 10 (dez) dias, os requisitos de infraestrutura para instalação da solução, o Plano de instalação, testes e ativação incluindo o Cronograma Detalhado de Execução dos Serviços, prevendo as datas de início e término da instalação de todos os licenciamentos.

2.9.4.6. O Cronograma da Contratada deverá ser submetido ao Departamento de Tecnologia da Informação er Comunicação - DTIC, observado o respectivo serviço e somente será válido após aprovação. Depois de validado, a Contratada será notificada para dar início à execução do cronograma aprovada pelo DTIC/Cofen.

2.9.4.7. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a Contratada sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo ao Contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

2.9.4.8. O fornecedor deverá entregar a solução instalada e customizada de acordo com os padrões fornecidos no Termo de Referência.

2.9.4.9. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos endpoints. Em momento anterior à instalação, o Contratante poderá solicitar os comprovantes da qualificação profissional do técnico que executará os serviços, podendo exigir a troca de profissional, caso este não satisfaça as condições supramencionadas.

2.9.4.10. O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico.

2.9.4.11. A console de gerenciamento deve oferecer também, opção para gerenciamento em nuvem, disponibilizado pela Contratada.

2.9.4.12. Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

2.9.4.13. Possibilidade de instalação dos clientes em estações de trabalho e servidores, podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).

2.9.4.14. Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores do Contratante.

2.9.4.15. Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.

2.9.4.16. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

2.9.4.17. A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

2.9.4.18. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).

2.9.4.19. A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos a não exclusivamente políticas, tarefas, e demais objetos do console.

2.10. **ITENS 16 e 19 – SOLUÇÃO DE CONECTIVIDADE LOCAL E WIRELESS**

2.10.1. **Serviço de Conectividade Local** - o serviço de conectividade local deve prover no mínimo os seguintes requisitos técnicos:

2.10.1.1. CARACTERÍSTICAS GERAIS

I - O serviço de conectividade deverá funcionar através do fornecimento de equipamentos de conectividade local com a disponibilização de switches de 48 portas físicas.

II - A Contratada deverá fornecer todos os softwares e licenciamentos necessários para atender as funcionalidades do serviço de conectividade local.

III - A Contratada deverá realizar o gerenciamento centralizado de todos os equipamentos, aplicando configurações e ações em tempo real.

IV - O gerenciamento deverá ser realizado via HTTPS, SSH e REST API.

V - Possibilitar o agrupamento dos equipamentos, de forma a permitir o gerenciamento de cada grupo de forma individualizada, com seleção de configurações de Vlans para cada grupo de pontos de acesso.

VI - O gerenciamento poderá estar direta e/ou remotamente conectado aos equipamentos por ele gerenciados, ou seja, conectados em diferentes redes e interligados por roteamento.

VII - Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil.

2.10.1.2. CARACTERÍSTICAS DO SWITCH

I - Possuir LEDs de identificação de atividades, de status do sistema, de cada porta, e de alimentação.

II - Possuir altura de no máximo 1U.

III - Permitir instalação em gabinete de 19″ (dezenove polegadas).

IV - Possuir 48 (quarenta e oito) portas “autosense” ou autonegociável 10/100/1000 com suporte a conectores RJ45 (10BASE-T de acordo com o padrão IEEE 802.3, 100BASE-TX de acordo com o padrão IEEE 802.3U e 1000BASE-T de acordo com o padrão 802.3ab).

V - Possuir 48 (quarenta e oito) portas full poe nos padrões 802.3af/802.3at.

VI - Possuir, no mínimo, 4 (quatro) portas 10 Gigabit Ethernet com suporte à inserção de transceivers do tipo SFP+.

VII - Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB ou RJ-45.

VIII - Capacidade de comutação de no mínimo 176 (cento e setenta e seis) Gbps de throughput.

IX - Possuir capacidade de armazenamento de no mínimo 32.000 (trinta e dois mil) endereços MAC.

X - Implementar a configuração de no mínimo 256 (duzentas e cinquenta e seis) VLANs simultaneamente.

XI - Implementar a configuração de no mínimo 4.000 (quatro mil) VLANs IDs.

XII - Possuir armazenamento para buffer de no mínimo 2 Mb.

XIII - Possuir autenticação 802.1x.

XIV - Possuir capacidade de coletar logs via syslog.

XV - Capacidade de aplicar listas ALC.

XVI - Capacidade de utilizar IEEE 802.1D MAC Bridging/STP (RSTP compatível).

XVII - Capacidade de utilizar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).

XVIII - Capacidade de utilizar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

XIX - Capacidade de utilizar Edge Port / Port Fast.

XX - Capacidade de IEEE 802.1Q VLAN Tagging.

XXI - Capacidade de Guest VLAN and Voice VLAN;

XXII - Capacidade de IEEE 802.3ad Link Aggregation com LACP.

XXIII - Capacidade de balanceamento de trafego sobre as portas trunk com Unicast e Multicast.

XXIV - Capacidade de implementar IEEE 802.1AX.

XXV - Capacidade de implementar Spanning Tree Instances (MSTP/CST).

XXVI - Capacidade de implementar IEEE 802.3x Flow Control and Back-pressure.

XXVII - Capacidade de implementar IEEE 802.3 10Base-T.

XXVIII - Capacidade de implementar IEEE 802.3u 100Base-TX.

XXIX - Capacidade de implementar IEEE 802.3z 1000Base-SX/LX.

XXX - Capacidade de implementar IEEE 802.3ab 1000Base-T.

XXXI - Capacidade de implementar IEEE 802.3bz Gigabit Ethernet support.

XXXII - Capacidade de implementar IEEE 802.3 CSMA/CD.

XXXIII - Capacidade de implementar Storm Control.

XXXIV
- Capacidade de implementar Port Mirroring;

XXXV - Capacidade de implementar DHCP Relay.

XXXVI
- Capacidade de implementar autenticação IEEE 802.1x baseado em portas.

XXXVII
- Capacidade de implementar IEEE 802.1x Guest VLAN.

XXXVIII
- Capacidade de implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).

XXXIX
- Capacidade de implementar IEEE 802.1ab LLDP-MED.

XL - Capacidade de implementar DHCP-Snooping.

XLI - Capacidade de implementar MAC Address Filtering.

XLII - Capacidade de implementar Priority Tag - Packet Ingress Filtering.

XLIII - Capacidade de implementar QoS usando IEEE 802.

XLIV - Capacidade de implementar QoS IP TOS/DSCP Based Priority Queuing.

2.10.2. **Serviço de Conectividade Wireless** - o serviço de conectividade wireless deve prover no mínimo os seguintes requisitos técnicos:

2.10.2.1. CARACTERÍSTICAS GERAIS

I - O Sistema de Gerenciamento Centralizado deverá funcionar através de controladora wireless, podendo ser appliance físico, virtual ou em nuvem este deve ser compatível com sistema de servidor virtual VMWare fornecida pelo Contratante.

II - A Contratada deverá fornecer todos os softwares e licenciamentos necessários para atender as funcionalidades do Sistema de Gerenciamento Centralizado, sem prazo de utilização ou de expiração de qualquer licença.

III - O sistema de gerenciamento Centralizado da Rede Sem Fio deverá realizar o gerenciamento centralizado de todos os pontos de acesso da rede sem fio, assim como gerenciar a conexão dos usuários conectados em tempo real.

IV - Disponibilizar interface web para a operação da controladora wireless acessível através de protocolo seguro https.

V - Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados.

VI - Suportar, gerenciar e controlar no mínimo a quantidade de Acess Points adquiridos.

VII - Os usuários não autenticados não deverão acessar a mesma Vlan dos usuários autenticados.

VIII - Implementar o protocolo IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: PEAP-MSCHAPv2.

IX - Integração com, no mínimo, 02 Servidores Radius que suporte os métodos EAP citados.

X - Possibilitar o agrupamento de Pontos de Acesso, de forma a permitir o gerenciamento de cada grupo de forma individualizada, com seleção de SSIDs, configurações de Vlans para cada grupo de pontos de Acesso.

XI - O Sistema de Gerenciamento Centralizado poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, ou seja, conectados em diferentes redes e interligados por roteamento. Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração. Possibilitar a criação de um novo SSID, definir os parâmetros de autenticação, definir as políticas de segurança associadas ao SSID, sem qualquer necessidade de acesso individual em cada Ponto de Acesso utilizado.

XII - Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de

traps. Permitir a gravação de eventos em log interno e/ou externo por meio de servidor de SYSLOG do Contratante. Possuir sistema de busca de informações do cliente a partir do endereço IP e endereço MAC.

XIII - Possuir Listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC.

XIV - Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC.

XV - Opção seleção automática do canal de rádio.

XVI - Implementar criptografia entre a comunicação do ponto de acesso e o sistema de gerenciamento centralizado.

XVII - Possibilitar, no mínimo, as seguintes formas de autenticação na rede sem fio:

a) Autenticação por chave pré-compartilhada (PSK), cada estação que se conectar no SSID deverá fornecer a chave pré-compartilhada para acessar os recursos de rede, devendo ser utilizado o protocolo WPA2, com algoritmo de criptografia AES, 128 bits;

b) Autenticação pelo padrão IEEE 802.1X através de autenticação Radius;

c) Deve possuir funcionalidade de isolar cliente;

d) Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso;

e) Possuir suporte a pelo menos 8 Vlans com suporte ao padrão IEEE 802.1q

XVIII - Implementar associação de Regras e de QoS por usuário, com base nos parâmetros da etapa de autenticação. Deve incluir todas as licenças necessárias para que o Ponto de Acesso seja suportado pela solução de gerenciamento

XIX - Capacidade de Implementar limitação de banda por usuário.

XX - Possuir VPN-SSL para possibilitar túnel dedicado de criptografia entre dispositivo e controladora.

XXI - Possuir VPN-IPSEC para possibilitar túnel dedicado de criptografia entre dispositivo e controladora.

XXII - Possuir duplo fator de autenticação OTP para usuários sendo disponibilizado automaticamente ao criar o usuário sem necessidade de licença adicional.

2.10.2.2. PONTO DE ACESSO

I - Possuir no mínimo 2(duas) interfaces IEEE 802.3 10/100/1000BaseT.

II - Suporte a Alimentação PoE (Power over Ethernet) no padrão 802.3at.

III - Possuir 1(uma) interface console RJ45.

IV - Deve possuir 1 rádio com frequência de 2.4GHz e 1 rádio com frequência de 5GHz.

V - Suporte a velocidades de no mínimo 1250Mbps em 5GHz e 400Mbps em 2.4GHz.

VI - Cada rádio deverá possuir, no mínimo, 3 antenas internas omnidirecionais, com ganho de, no mínimo, 4.7 dBi para 2.4 GHz e 5.9 dBi para 5 GHz.

VII - Suporte a operação 3x3:3 MU-MIMO.

VIII - Suporte aos padrões IEEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, permitindo o uso simultâneo de usuários configurados em qualquer um dos padrões suportados.

IX - Possuir tecnologia 802.11ac WAVE2.

X - Suportar a utilização de canais de 20 e 40MHz.

XI - Suporte no mínimo 8 SSID’s simultâneos em cada rádio, com configurações independentes.

XII - Possuir LED para a indicação do status de funcionamento do equipamento.

XIII - Deve possibilitar a configuração de forma centralizada através de solução de gerenciamento que integre todos os pontos de acesso do ambiente, ou seja, o ponto de acesso receberá todas as configurações da rede sem fios através do sistema de gerenciamento centralizado.

XIV - Deve permitir a comunicação com o sistema de gerenciamento por IP, sem a necessidade de utilizar a mesma VLAN.

XV - Possuir certificações Anatel, CB, UL, CE, FCC, ISED (IC), RCM, EN 60601-1-2 (Medical Equipment Directive), Plenum-rated (UL2043).

XVI - Possuir mecanismo de segurança contra furto do tipo "Kensington security lock point" ou similar.

XVII - Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer todos os acessórios para que o serviço de instalação do ponto de acesso possa ser realizado.

XVIII - Injetor de energia.

XIX - Fornecer alimentação elétrica dos APs via interface de rede 10/100/1000, de acordo com o padrão PoE (Power over Ethernet Plus), mantendo todas as suas funcionalidades e capacidade, calculados para o desempenho máximo do AP, ou seja, todos os transmissores e receptores que compõem o AP.

XX - Os Pontos de Acesso não poderão sofrer nenhum tipo de perda, seja performance, transmissão ou qualquer funcionalidade quando alimentado por Power over Ethernet Plus (PoE) conforme o padrão 802.3af.

XXI - Deverá possuir fonte de alimentação com seleção automática de tensão (100 – 240 VAC).

XXII - Deverá ser específico para ambiente interno.

XXIII - Deverá fornecer no mínimo 20W.

XXIV - Deverá ser acompanhado de cabo de energia necessário para sua operacionalização.

2.10.3. **Serviços Comuns à Solução de Conectividade Local e Wireless**

2.10.3.1. Os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços de conectividade wireless deverão ser instalados no ambiente do Contratante, sob demanda, em lotes mínimos de 10 access points e switches.

2.10.3.2. Os serviços deverão observar os seguintes requisitos mínimos:

I - Serão realizados em todos os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço, em regime 24x7 (24 horas por dia, sete dias por semana).

II - Comunicar ao Contratante a existência do patch juntamente com os respectivos problemas resolvidos e as novas funcionalidades disponibilizadas. A periodicidade dessa comunicação será definida pelo Contratante na reunião de início do projeto (kick-off).

III - Atualizar os módulos da solução, isto é, fornecer e instalar patches, correções e versões ou releases mais recentes dos softwares.

IV - Executar procedimentos, resolver problemas e esclarecer dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento dos módulos.

V - Executar atividades de suporte, manutenção e resolução de problemas e de configuração, de cada um componentes dos serviços, remotamente.

VI - Realizar o ajuste fino (tunning) de toda a solução, adequando-a ao ambiente do Contratante e às customizações de configuração necessárias para atender às necessidades do Contratante.

VII - Resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da solução.

VIII - Será permitida a prestação dos serviços por meio de:

a) Estabelecimento de VPN em links internet alocados pela Contratada exclusivamente para essa conexão ou estabelecimento de VPN em links SLDD alocados pela Contratada exclusivamente para essa conexão;

b) Caso seja necessária a utilização de elementos adicionais para o estabelecimento da VPN, estes devem ser alocados pela Contratada.

IX - Avaliar periodicamente a customização dos softwares de gerência da Contratada, incluindo os alarmes de todos os componentes e ajuste de suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas no console de gerência.

X - Os elementos instalados nas dependências do Contratante devem:

a) possuir fonte de alimentação 110/220V;

b) ser fixados em rack padrão 19 (sempre que aplicável).

XI - Verificar, diariamente, a disponibilização, pelo fabricante, de patches, correções e versões ou releases mais recentes dos softwares.

2.10.3.3. PLANEJAMENTO, CUSTOMIZAÇÃO DE AMBIENTE E INSTALAÇÃO DE ATIVOS DE REDE

I - A Contratada deverá atender as seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de projeto executivo, planejamento de atividades de instalação, customização de ambiente, migração tecnológica e ativação de serviços, sem ônus adicionais para o Contratante:

a) serão de responsabilidade da Contratada as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, em conformidade com o projeto executivo a ser elaborado e apresentado pela Contratada para aprovação pelo Contratante;

b) caso os produtos alocados venham a substituir solução existente no Contratante, caberá à Contratada levantar a configuração atual e fazer a migração das configurações existentes para a solução utilizada no provimento dos serviços;

c) a Contratada deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do projeto executivo e, se pertinente, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;

d) as visitas poderão ser realizadas nos dias úteis, das 08h as 14h, mediante agendamento prévio com a unidade responsável;

e) Independentemente da alocação dos racks pela Contratada, esta deverá efetuar a reorganização dos racks existentes, de forma a acomodar os seus equipamentos;

f) As atividades de migração e mudanças deverão ocorrer de acordo com as políticas adotadas pela equipe técnica do Contratante;

g) as definições de Migração e Mudanças serão realizadas por meio de reuniões online com periodicidade semanal. As reuniões previstas semanalmente são exatamente para avaliar a necessidade e quantidade das mudanças e migrações, caso ocorram.

h) nessas reuniões serão aprovadas ou vetadas mudanças no ambiente operacional que porventura venham a causar indisponibilidade ou impactos no desempenho dos serviços de TI;

i) nas referidas reuniões participarão os funcionários do Contratante responsáveis pela disponibilização e manutenção da infraestrutura de TI do órgão;

j) o técnico responsável pelas atividades da Contratada deverá participar das reuniões de Migração e Mudanças para exposição dos riscos associados.

II - A elaboração do Projeto Executivo ficará a cargo da Contratada e deverá atender as seguintes condições:

a) conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase, respeitando os prazos;

b) detalhar a ementa dos treinamentos a serem ministrados.

III - Os equipamentos, softwares e demais componentes necessários à correta prestação dos serviços deverão:

a) ser entregues, instalados e configurados nas dependências do Contratante;

b) conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional do Contratante e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;

c) conter a última versão de software e firmware disponibilizada pelo fabricante;

d) ter configuradas senhas de acesso para que a equipe de funcionários

designada pelo Contratante efetue o acesso para a visualização das configurações e logs;

e) ter configurada senha com direitos totais de administração e configuração a ser utilizada pelo Contratante em caso de emergência;

f) ser configurados para enviar logs para as soluções de concentração de logs disponibilizados no site central e de contingência do Contratante;

g) ser configurados para gerenciamento SNMP versões 1 e 2 por meio da solução em uso no Contratante;

h) para aprovação da instalação e configuração de qualquer item que enseje a emissão de termo de recebimento definitivo, a Contratada deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

i) as atividades quando realizadas no ambiente de produção poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 18h ou em finais de semana e feriados).

IV - Após a instalação, a Contratada deverá realizar operação assistida para os serviços contratados. A operação assistida deverá obedecer aos requisitos abaixo:

a) iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pelo Contratante que seja feita em data diferente;

b) será executada nas dependências do Contratante, em horário de expediente;

c) caso seja necessária a consecução de atividades, pelo técnico responsável pela operação assistida, que possam afetar a disponibilidade de serviços de rede do Contratante, estas devem ocorrer após às 18h;

d) caso o Contratante encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

e) caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade da Rede do Contratante, a Contratada deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

V - A Contratada deverá implementar e documentar para todos os componentes da solução as configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening) como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários-padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.

2.11. **ITENS 17 e 20 – INSTALAÇÃO DA SOLUÇÃO DE CONECTIVIDADE LOCAL E WIRELESS**

2.11.1. Instalação de equipamentos Access Points e Switches, bem como do software para gerenciamento centralizado destes equipamentos.

2.11.2. A Contratada deverá oferecer implantação das soluções, com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato e de acordo com as regras e políticas exigidas pela equipe técnica do Contratante, dentro do escopo das funcionalidades, de cada serviço, definidas neste Termo.

2.11.3. Deverão ser apresentados os seguintes entregáveis durante a implantação:

2.11.3.1. Fase de desenho da arquitetura.

2.11.3.2. Esquema detalhado de conexão com dispositivos.

2.11.3.3. Fase de instalação.

2.11.3.4. Envio de resumo com atividades realizadas, avanços e problemas detectados.

2.11.3.5. Fase de pós instalação.

2.11.4. A Contratada confeccionará relatório(s) final(is) sobre as atividades realizadas e recomendações

ao Contratante. Este relatório será entregue 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

2.11.4.1. Introdução;

2.11.4.2. Análise do ambiente;

2.11.4.3. Atividades realizadas;

2.11.4.4. Configuração de políticas aplicadas;

2.11.4.5. Conclusões.

2.11.5. Todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos do Contratante.

2.11.6. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados).

2.11.7. A Contratada será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do Contratante, sem prejuízo aos serviços desta.

2.11.8. Quando previamente acordado entre as partes, a Contratada poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante da instituição.

2.11.9. A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executada pela Contratada nos prédios do Contratante.

2.11.10. Deve abranger a instalação física e lógica da solução, em sua totalidade, com duração máxima de 60 (sessenta) dias corridos, compreendendo, mas não se limitando a essas, as seguintes atividades:

2.11.10.1. Instalação física dos equipamentos nas dependências do Contratante.

2.11.10.2. Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sentido de melhorar o gerenciamento e performance e aplicar os “patchs” para atualização do sistema, quando necessário.

2.11.10.3. Definição das funcionalidades a serem implantadas.

2.11.10.4. Definição da parametrização.

2.11.10.5. Instalação e configuração de toda a solução com vista ao gerenciamento dos recursos solicitados neste Termo em sua totalidade.

2.11.10.6. Os serviços de instalação e configuração deverão ser prestados nas dependências do Contratante.

2.11.11. É responsabilidade da Contratada quaisquer danos físicos aos equipamentos, durante os processos de instalação e configuração.

2.11.12. É proibida a divulgação de quaisquer aspectos da configuração desses equipamentos, por questões de sigilo e segurança, por parte dos técnicos responsáveis pela instalação e configuração, ou quaisquer outros que tenham acesso a essas informações, salvo quando houver autorização por escrito do Contratante).

2.11.13. Todas as senhas criadas e os usuários cadastrados nos processos de instalação e configuração dos equipamentos devem ser registrados e entregues por escrito ao responsável técnico indicado pelo Contratante.

2.11.14. Deverá ser entregue ao responsável técnico indicado pelo Contratante relatório com todos os procedimentos e configurações executados, assinado pelo responsável técnico da Contratada.

2.11.15. O início dos serviços deve ocorrer, no máximo, em 72 (setenta e duas) horas úteis, contadas a partir da assinatura do contrato.

2.11.16. A Contratada da solução deve executar, prioritariamente, como parte obrigatória do processo de instalação, as seguintes atividades:

2.11.16.1. Configuração da console de gerenciamento.

2.11.16.2. Migração das regras existentes na solução de segurança atual do Contratante.

2.11.16.3. Configuração da autenticação de usuários integrada ao domínio da rede “Microsoft”, via ferramenta nativa de integração da solução.

2.11.16.4. Análise de falsos positivos que podem ser gerados após implantação.

2.11.16.5. Adequações pós-instalação.

2.11.16.6. Instalação e configuração do concentrador de “logs”, “archive” e relatórios.

2.11.16.7. Migração, adequação e definição, juntamente com a equipe de Tecnologia da Informação do Contratante, das políticas para controle de tráfego de entrada e saída de dados.

2.11.16.8. Execução de testes de segurança através da análise de vulnerabilidades completa do perímetro de internet.

2.12. **ITENS 08, 15, 18 e 21 – SERVIÇOS DE TREINAMENTO**

2.12.1. Quando solicitado, deverá ser realizado treinamento para repasse de conhecimento à equipe do Contratante, contemplando no mínimo:

2.12.1.1. Práticas de gerenciamento e troubleshooting da solução instalada.

2.12.1.2. Material didático de cada solução implementada.

2.12.1.3. Cada treinamento poderá ser realizado em até duas turmas, uma vez que o máximo de participantes permitido por turma são 10 (dez) pessoas.

2.12.1.4. Os treinamentos deverão ter as seguintes cargas horárias:

a) Item 8 - Treinamento da Solução de Serviços Gerenciados de Firewall: 40 horas;

b) Item 15 - Treinamento da Solução de Endpoints: 20 horas;

c) Item 18 - Treinamento da Solução de Conectividade Local: 16 horas;

d) Item 21 - Treinamento da Solução e Conectividade Wireless: 16 horas.

2.12.2. O Contratante, cederá somente a sala, os computadores e o datashow (projetor) para o curso, podendo ser ministrado de forma remota.

2.12.3. Todos os custos referentes ao repasse de conhecimento deverão está incluso no valor global do contrato.

ANEXO C

PROVA CONCEITO

1. **OBJETIVO**

1.1. Ao final da fase de homologação documental, se o Contratante julgar necessário, o proponente será convocado para a homologação em laboratório, sendo prerrogativa do Contratante a análise de quais itens serão avaliados em laboratório.

1.2. A prova de conceito visa verificar se a licitante classificada para fornecer o objeto desta contratação demonstra sua capacidade de atendimento aos requisitos exigidos no Edital, Termo de Referência e Anexos, devendo comprovar um conjunto de capacidades que serão descritas no roteiro abaixo.

1.3. O não comparecimento da licitante na data e horário agendado pelo pregoeiro implica a desqualificação para a continuidade no certame.

1.4. O proponente deve dispor do objeto arrematado com toda a infraestrutura necessária para demonstrar, empiricamente, todas suas funcionalidades, em consonância com os itens do edital.

1.5. Para homologação em laboratório, o proponente deverá apresentar um plano de testes (conforme descrito no fim deste anexo), a ser enviado em até 5 (cinco) dias corridos após a convocação, descrevendo atividades, topologias/arquitetura e as configurações necessárias para a comprovação dos requisitos exigidos na especificação técnica, o que deverá ser validado pelo Contratante.

1.6. Após o recebimento do plano de testes pela equipe técnica do Contratante, será acordada a realização de reunião prévia (kick-off) com os representantes da empresa arrematante e o corpo técnico do Contratante, a fim de se definir a ordem e estratégia de execução dos testes, acordar horários e regras para os dias da homologação em laboratório.

1.7. O proponente deverá confeccionar e dispor, no ambiente de laboratório, de todos os elementos necessários à validação dos requisitos da solução ofertada e exigidos no edital, tais como, por exemplo: gerador de tráfego, gerador de ataques, ambientes promíscuos, contêineres, firewalls, MTA, servidores virtuais e cabos.

1.8. O proponente deverá efetuar a demonstração de que a solução atende aos itens técnicos do edital pelo prazo de até 15 (quinze) dias corridos, a contar da data seguinte à disponibilização da amostra (homologação em ambiente do Contratante) ou disponibilização do ambiente de testes (homologação virtual) e do completo repasse de informações pela Contratado ao Contratante sobre o funcionamento e manuseio da solução ofertada. Esse prazo pode, a critério do Contratante, ser prorrogado por mais 10 (dez) dias, em caso de necessidade de verificação mais detalhada.

1.9. Caso, durante a realização dos testes de bancada, seja constatada a dificuldade em se demonstrar algum dos itens desta especificação técnica, o proponente terá o prazo de até 2 (dois) dias úteis, contados da comunicação do fato, para solucionar o problema. A correção não deve envolver atualizações de softwares, patches, novas versões do produto, sendo permitido apenas reconfigurações da solução já entregue e instalada.

1.10. Os testes de homologação serão executados por técnicos do proponente e/ou do fabricante da solução ofertada, acompanhados pela equipe técnica do Contratante. Toda a coleta de evidências e preenchimento do documento “modelo de plano de testes” é de responsabilidade do proponente.

1.11. Quanto ao acompanhamento da homologação de laboratório por interessados, estes devem manifestar formalmente o interesse, via e-mail para ti@cofen.gov.br, no prazo de até 2 (dois) dias úteis após a convocação para apresentação do plano de testes.

1.12. Para acompanhamento da homologação, será permitido um representante de cada empresa participante da licitação e somente sob a condição de observador. Será permitida a presença de representante do fabricante da solução ofertada durante a análise da amostra.

1.13. Não será permitida, no momento de homologação, a interação entre os ouvintes com quaisquer participantes. Questões sobre o processo deverão seguir os trâmites de contato via responsável pela homologação e em momento oportuno.

1.14. A critério do Contratante, a homologação da amostra em ambiente de laboratório poderá ocorrer de 2 (duas) maneiras:

1.14.1. Homologação em ambiente interno do Contratante: entende-se como a localidade interna do Contratante, onde há recursos tecnológicos que propiciem ao proponente condições de montar o ambiente necessário à comprovação dos itens exigidos no edital. É prerrogativa do Contratante prover apenas a infraestrutura necessária, compreendendo as bancadas, energia elétrica estabilizada, link de internet e condicionamento de ar.

1.14.1.1. O proponente deverá comparecer presencialmente, em local indicado no edital, podendo este ser negociado, quando o Contratante julgar necessário, para fins de adequação às características distintas que a tecnologia arrematada possa exigir na sua comprovação.

1.14.1.2. A amostra deverá ser entregue em até 15 (quinze) dias corridos, contados da data da convocação, podendo ser prorrogado por mais 15 (quinze) dias corridos, desde que justificado e aceito pelo Contratante.

1.14.1.3. Após o prazo de entrega do exemplar, não será permitido ao proponente a substituição, total ou parcial, ou a entrega de novos exemplares.

1.14.2. Homologação em ambiente externo ao do Contratante: entende-se como sendo a homologação realizada em ambiente externo à localidade do Contratante, podendo ser realizado em ambiente do proponente.

1.14.3. Todo o processo ocorrerá em ambiente criado pelo proponente, com toda a infraestrutura necessária a comprovação dos itens do edital. Para disponibilização do ambiente de laboratório e início dos testes de homologação, a Licitante terá o prazo de até 15 (quinze) dias corridos, após a reunião de kickoff.

1.14.4. A homologação em ambiente externo ao do Contratante poderá ser realizada de forma presencial em local definido pelo proponente, caso haja algum impeditivo técnico para sua realização no ambiente interno do Contratante.

1.15. A homologação poderá, a critério do Contratante, ser realizada de forma virtual, com transmissão pela internet. O proponente ficará responsável por prover meios para a transmissão via áudio e vídeo.

1.16. A transmissão deve viabilizar a interação entre analistas do Contratante e os representantes do time técnico do proponente, permitindo a visualização dos elementos utilizados na homologação, compartilhamento de telas e demonstração de comprovação dos elementos.

1.17. O meio de transmissão deverá ser disponível a outros licitantes ou interessados que queiram participar da homologação, sem limite de expectadores, desde que solicitado ao responsável pela licitação a intenção de acompanhar essa fase do certame.

1.18. É vedado aos participantes da homologação gravar a transmissão com pena de violação legal de propriedade intelectual.

1.19. Caso ocorram problemas na transmissão, que dificultem a visualização da homologação, o Contratante poderá, em acordo com o proponente, avaliar um prazo para solução. Se o problema persistir, a homologação deverá seguir em ambiente do Contratante, conforme rege este documento.

1.20. No momento da homologação, o Contratante não emitirá juízo de valor quanto ao atendimento ou não de um item. Os analistas do Contratante poderão se manifestar para sanar dúvidas quanto a apresentação da comprovação do item.

1.21. Em até 5 (cinco) dias corridos após a finalização dos testes de homologação, o proponente deverá encaminhar as evidências de atendimento dos testes ao e-mail ti@cofen.gov.br.

1.22. Após o recebimento das evidências dos testes de bancada, os técnicos do Contratante irão elaborar um laudo com registros dos testes realizados, indicando se a solução foi ou não homologada.

1.23. Se não aprovado, o pregoeiro dará continuidade ao certame licitatório convocando os demais licitantes, por ordem de classificação final da etapa de lances, com o objetivo de cumprir os requisitos do termo de referência.

MODELO DE PLANO DE TESTES PARA HOMOLOGAÇÃO

Logo e nome da empresa proponente	PREGÃO ELETRÔNICO Nº xxxx/xxxx	Revisão: 01
	CARDENO DE TESTES	Página: 1/1

I - CADERNO DE TESTES: Serviços Gerenciados e Integrados de Segurança e Serviços de Conectividade Wireless e local

a) Descrição do processo licitatório, por exemplo: *"Homologação Pregão Eletrônico Nº.XXXX/XXXX"*

II - SUMÁRIO: Nele deve conter sumário descritivo das informações do processo e etapas da homologação.

III - OBJETIVO DO CADERNO DE TESTE: Nele deve conter a descrição breve do objetivo deste Caderno, conforme exemplo abaixo.

a) "*Este caderno de testes faz referência ao item XX do termo de referência do certame XXXX/XXXX, que visa comprovar as funcionalidades e requisitos técnicos Da solução XYZ"*

IV - ESTRUTURA FÍSICA: Mostrar a estrutura física que será utilizada para comprovação dos testes relacionados no anexo do Edital. Informar os equipamentos ou softwares virtuais que serão entregues para homologação contendo no mínimo as informações: "Quantidade", "Modelo de Equipamento" e "Descrição"), conforme exemplo abaixo.

a)

Quantidade	*Modelo Equipamento*	Descrição
2	*Firewalls ABC*	*NFGW+IPS*
1	*Switch XYZ*	*Para conexão dos elementos de rede*
1	*Servidor Alfa*	*Servidor para teste do ambiente de Virtualização*
1	*Gerador de tráfego*	*Por exemplo: "Spirent"*

b) *"Cabeamentos: Cabos UTP cat. 6*; "*Transceivers XYZ*"

V - AMBIENTE DE TESTE: Submeter desenho da topologia lógica que será utilizada na realização dos testes. Descrever o ambiente configurado com informações tais como, endereços de rede, regras da solução implementada, NATs, controles de aplicações, assinaturas, geração de logs e demais informações relevantes a realização dos testes relativos ao objeto licitado), conforme exemplo abaixo.

a) *"Introdução: para execução dos testes será utilizado uma estrutura de ambiente em formato XYZ, composta por uma LAN, WAN e o elemento k (objeto da licitação) configurado com as seguintes regras: abc, xyz e os endereços klm"*

VI - RELATÓRIO FINAL: Deve conter as informações de referência do item do Edital ou item da folha de testes que está sendo avaliado, conter o objetivo do teste a configuração utilizada e o procedimento

adotado para realização), conforme exemplo abaixo:

a) *"Cada item do Edital ou da folha de testes deve ser evidenciado na formatação descrita abaixo:*

Data da realização do teste:	
Item x.y.z do edital	*A solução de firewall deve possuir throughput de 4 (quatro) Gbps com IPS habilitado.*
Objetivo do Teste	*Verificar os índices de throughput.*
Configuração do Teste	*Configurados profiles de Sensor de IPS com as assinaturas ativas.*
Procedimento do Teste	*Gerar tráfego a partir do gerador de tráfego para fazer match na regra com os itens habilitados.*
Evidências	*"Print de tela" ou conforme documentação do fabricante*
Anotações	
Conformidade do adquirente	

ANEXO D

NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

1. DESCRIÇÃO

1.1. Os serviços devem ser prestados no prazo máximo de 24 (vinte e quatro) horas, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pelo Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela Contratada e autorizado pelo Contratante.

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

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

1.4. Na execução de todos os serviços, deverão ser observados os seguintes prazos indicados na tabela abaixo:

Severidade	Atividade, Tarefa ou Serviço	Prazo Máximo de Início de Atendimento	Prazo Máximo de Solução de Problema
Emergencial	São consideradas como "emergência" todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Exemplo: situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente, parcial ou total de serviços ou perda de tráfego.	15 (quinze) minutos	4 (quatro) horas
Grave	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento. São problemas sérios ou perturbações que afetam uma área específica ou determinada funcionalidade do equipamento. Exemplo: perda de redundância, reinicialização de	15 (quinze) minutos	6 (seis) horas

	módulos, slots ou portas com defeitos, degradação de desempenho, perda de funcionalidades.		
Pedido de Informação	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis de configurações ou usos que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica.	15 (quinze) minutos	24 (vinte e quatro) horas

1.5. Todos os prazos para resolução de incidentes ou eventos especificados na tabela acima são contados a partir da abertura do respectivo número de identificação do chamado ou ticket.

1.6. A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pelo Contratante com o número fornecido pela Contratada.

1.7. Os atendimentos poderão ser atendidos de forma remota, sempre respeitando o estabelecido no presente NMS;

1.8. No momento de abertura do chamado, deverá ser fornecido ao Contratante um número único de identificação e o chamado deverá ser classificado, pela Contratada, conforme o estabelecido no Anexo D - Níveis Mínimos de Serviço (NMS). A classificação do chamado está sujeita a alteração pelo Contratante, sempre que este julgar necessário. Neste caso, os tempos de atendimento e resolução serão contados a partir do momento em que o Contratante efetuar a solicitação de alteração de prioridade.

1.8.1. No caso de chamado classificado em sua abertura, pelo Contratante, segundo o nível de severidade identificado pelos técnicos do DTIC, não poderá ser reclassificado durante o atendimento pela Contratada. E nesse caso, o prazo definido para início do atendimento e resolução do problema, deverá ser aquele correspondente a classificação de severidade definido inicialmente em sua abertura.

1.9. A Contratada deverá cumprir com as seguintes atividades considerando os requisitos temporais apresentados:

1.9.1. Mobilizar e apresentar toda a equipe técnica de manutenção em até 5 (cinco) dias após a assinatura do Contrato Administrativo, formalizando junto ao Contratante por meio de documento escrito;

1.9.2. Os serviços devem ser prestados de forma contínua, em tempo integral durante a vigência contratual, sempre de forma proativa e respeitando os prazos estabelecidos neste NMS, quando da abertura de chamados técnicos/tickets; e

1.9.3. Elaborar o relatório mensal de prestação dos serviços contendo todas as atividades realizadas no período.

ANEXO E

MODELO DE DECLARAÇÃO DE ATENDIMENTO AOS CRITÉRIOS DE SUSTENTABILIDADE SOCIOAMBIENTAL

Nome empresarial da licitante:

Inscrição no CNPJ nº:

Endereço completo da sede:

Nome do representante legal:

Carteira de Identidade nº:

CPF nº:

Por intermédio de seu representante legal infra-assinado, para atendimento ao disposto no item 4.16 do Termo de Referência, constante do presente Processo Cofen SEI, DECLARA, sob as penas da Lei nº 6.938/1981 e demais normativos pertinentes, expressamente que:

a) Atende aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de

proteção do meio ambiente, em conformidade com o estabelecido no item 4.16 do Termo de Referência, com a Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos), com a IN 01/2010-SLTI, com a Instrução Normativa n° 6, de 24 de março de 2014, do IBAMA, e outras aplicáveis ao objeto em questão.

b) Não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas à escravidão, instituído pela Portaria Interministerial MTPS/MMIRDH n. 04 de 11/05/2016;

c) Não foi condenada, a Contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988, do art. 149 do Código Penal Brasileiro, do Decreto n. 5.017/2004 (promulga o Protocolo de Palermo) e das Convenções da OIT n. 29 e 105.

Por ser expressão da verdade, firma-se a presente.

Brasília, _____ de _____ de 2024.

Nome completo do Representante Legal _____

Assinatura _____

ANEXO F

MODELO DE DECLARAÇÃO DE VISTORIA

Nome empresarial da licitante:

Inscrição no CNPJ nº:

Endereço completo da sede:

E-mail:

Telefone:

Nome do representante legal:

Carteira de Identidade nº:

CPF nº:

Declaro que vistoriei minuciosamente os locais para a prestação dos serviços constantes do objeto do Edital de Licitação nº _____/20___, e tomei conhecimento das reais condições de execução dos serviços, bem como coletei informações de todos os dados e elementos necessários à perfeita elaboração da proposta comercial.

(Obs. Enviar preenchido e assinado com cópia autenticada da procuração se for o caso)

Brasília, _____ de _____ de 2024.

Nome completo do Representante Legal _____

Assinatura _____

ANEXO G

MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO E SIGILO E DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO DE MANUTENÇÃO E SIGILO

Este Termo de Compromisso é celebrado entre:

CONTRATANTE, o **Conselho Federal de Enfermagem (Cofen)**, sediado no BL E - SCLN QD 304, LOTE 09 - Asa Norte, Brasília/DF, inscrito no CNPJ/MF **47.217.146/0001-57** , neste ato representada por seus respectivos procuradores abaixo assinados, na forma de seus respectivos Contratos Sociais, e CONTRATADA <**NOME DA EMPRESA**>, sediada em <ENDEREÇO>, inscrita no CNPJ n° <**Nº do CNPJ**>, neste ato representada por seus respectivos procuradores abaixo assinados, na forma de seus respectivos Contratos Sociais.

O Órgão e a Empresa podem ser referidos individualmente como Parte e coletivamente como Partes, onde o contexto assim o exigir.

CONSIDERANDO QUE as Partes estabeleceram ou estão considerando estabelecer uma relação de negócio que possa incluir, entre outras, uma ou mais das seguintes relações ("Relação"): serviços de marketing, consultas, pesquisa e desenvolvimento, fornecimento/venda, teste/ensaio, colaboração, agenciamento, licitação, ou qualquer outra parceria que envolva a divulgação de Informações Confidenciais de uma Parte a outra;

CONSIDERANDO QUE as Partes podem divulgar entre si Informações Confidenciais, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios, e em consideração da divulgação destas Informações Confidenciais; e

CONSIDERANDO QUE as Partes desejam ajustar as condições de revelação das Informações Confidenciais, bem como definir as regras relativas ao seu uso e proteção.

1. Para a finalidade deste Termo, "Informações Confidenciais" significarão todas e quaisquer informações divulgadas por uma Parte (de acordo com este instrumento, a "Parte Divulgadora") à outra Parte (de acordo com este instrumento, a "Parte Recebedora"), em forma escrita ou verbal, tangível ou intangível, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, a qual esteja claramente marcada como CONFIDENCIAL, incluindo, entre outras, mas não se limitando a, segredos comerciais, know-how, patentes, pesquisas, planos de negócio, informações de marketing, informações de clientes, situação financeira, métodos de contabilidade, técnicas e experiências acumuladas, e qualquer outra informação técnica, comercial e/ou financeira, seja expressa em notas, cartas, fax, memorandos, acordos, termos, análises, relatórios, atas, documentos, manuais, compilações, código de software, e-mail, estudos, especificações, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, disquetes, fitas, pareceres e pesquisas, ou divulgadas verbalmente e identificadas como confidenciais por ocasião da divulgação.

2. Não serão incluídas nas Informações Confidenciais quaisquer informações que: (i) sejam geralmente conhecidas, ou subsequentemente se tornem disponíveis ao comércio ou ao público; (ii) estejam na posse legal da Parte Recebedora antes da divulgação pela Parte Divulgadora; ou (iii) sejam legalmente recebidas pela Parte Recebedora de um terceiro, desde que essas informações não tenham chegado ao conhecimento da Parte Recebedora através do referido terceiro, direta ou indiretamente, a partir da Parte Divulgadora numa base confidencial.

3. Quando a divulgação de Informações Confidenciais for necessária para estrito atendimento de ordem judicial ou agência governamental, o mesmo se procederá da seguinte maneira: (i) a Parte Recebedora fica obrigada a comunicar o teor da determinação judicial à Parte Divulgadora no prazo de 2 (dois) dias úteis a contar do recebimento da ordem, no caso de se tratar de determinação para cumprimento em prazo máximo de 5 (cinco) dias; ou no prazo de uma hora a contar do recebimento, no caso de se tratar de ordem judicial para cumprimento no prazo máximo de até 48 (quarenta e oito) horas; e (ii) fica a Parte Recebedora obrigada também a enviar a Parte Divulgadora cópia da resposta dada à determinação judicial ou administrativa concomitantemente ao atendimento da mesma. A Parte Recebedora cooperará com a Parte Divulgadora para possibilitar que a Parte Divulgadora procure uma liminar ou outra medida de proteção para impedir ou limitar a divulgação dessas Informações Confidenciais.

4. A Parte Recebedora não divulgará nenhuma Informação Confidencial da Parte Divulgadora a nenhum terceiro, exceto para a finalidade do cumprimento deste Termo e com o consentimento prévio por escrito da Parte Divulgadora. Além disso:

a) A Parte Recebedora, (i) não usará as Informações Confidenciais para interferir, direta ou indiretamente, com nenhum negócio real ou potencial da Parte Divulgadora, e (ii) não usará as Informações Confidenciais para nenhuma finalidade, exceto avaliar uma possível relação estratégica entre as Partes;

b) As Partes deverão proteger as Informações Confidenciais que lhe forem divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias Informações Confidenciais;

c) A Parte Recebedora não revelará, divulgará, transferirá, cederá, licenciará ou concederá acesso a essas Informações Confidenciais, direta ou indiretamente, a nenhum terceiro, sem o prévio consentimento por escrito da Parte Divulgadora, estando este terceiro, condicionado à assinatura de um Termo de Compromisso de Manutenção de Sigilo prevendo as mesmas condições e obrigações estipuladas neste Termo;

d) A Parte Recebedora informará imediatamente a Parte Divulgadora de qualquer divulgação ou uso não autorizado das Informações Confidenciais da Parte Divulgadora por qualquer pessoa, e tomará todas as medidas necessárias e apropriadas para aplicar o cumprimento das obrigações com a não-divulgação e uso limitado das obrigações das empreiteiras e agentes da Parte Recebedora;

e) A Parte Recebedora deverá manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou Informações Confidenciais, devendo comunicar à Parte Divulgadora, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade; e

f) A Parte Recebedora obrigará seu pessoal que possa ter acesso às Informações Confidenciais que cumpram tais obrigações de sigilo

5. As Partes se comprometem e se obrigam a tomar todas as medidas necessárias à proteção da informação confidencial da outra Parte, bem como para evitar e prevenir revelação a terceiros, exceto se devidamente autorizado por escrito pela Parte Divulgadora. De qualquer forma, a revelação é permitida para empresas coligadas, assim consideradas as empresas que direta ou indiretamente controlem ou sejam controladas pela Parte neste Termo. Além disso, cada Parte terá direito de revelar a informação a seus funcionários que precisem conhecê-la, para os fins deste Termo; tais funcionários deverão estar devidamente avisados acerca da natureza confidencial de tal informação, e estarão vinculados aos termos e condições do presente Termo de Compromisso de Manutenção de Sigilo independentemente de terem sido avisados do caráter confidencial da informação, ficando a Parte Recebedora responsável perante a Parte Divulgadora por eventual descumprimento do Termo.

6. O intercâmbio de informações nos termos deste instrumento não será interpretado de maneira a constituir uma obrigação de uma das Partes para celebrar qualquer Termo ou acordo de negócio, nem obrigarão a comprar quaisquer produtos ou serviços da outra ou oferecer para a venda quaisquer produtos ou serviços usando ou incorporando as Informações Confidenciais.

7. Cada Parte reconhece que em nenhuma hipótese este Termo será interpretado como forma de transferência de propriedade ou qualquer tipo de direito subsistido nas Informações Confidenciais da Parte Divulgadora para a Parte Recebedora, exceto o direito limitado para utilizar as Informações Confidenciais conforme estipulado neste Termo.

8. Este Termo entrará em vigor por ocasião da assinatura pelas Partes. Os compromissos deste instrumento também serão obrigatórios às coligadas, subsidiárias ou sucessoras das Partes e continuará a ser obrigatório a elas até a ocasião em que a substância das Informações Confidenciais tenha caído no domínio público sem nenhum descumprimento ou negligência por parte Recebedora, ou até que a permissão para liberar essas Informações seja especificamente concedida por escrito pela Parte Divulgadora.

9. A omissão ou atraso em aplicar qualquer disposição deste Termo não constituirá uma renúncia de qualquer aplicação futura dessa disposição ou de quaisquer de seus termos. Se qualquer disposição deste Termo, ou sua aplicação, por qualquer razão e em qualquer medida for considerada inválida ou inexequível, o restante deste Termo e a aplicação de tal disposição a outras

pessoas e/ou circunstâncias serão interpretados da melhor maneira possível para atingir a intenção das Partes signatárias.

10. As Partes concordam que a violação do presente Termo, pelo uso de qualquer Informação Confidencial pertencente à Parte Divulgadora, sem sua devida autorização, causar-lhe-á danos e prejuízos irreparáveis, para os quais não existe remédio na lei. Desta forma, a Parte Divulgadora poderá, imediatamente, tomar todas as medidas extrajudiciais e judiciais, inclusive de caráter cautelar, como antecipação de tutela jurisdicional, que julgar cabíveis à defesa de seus direitos.

11. A Parte Recebedora deverá devolver, íntegros e integralmente, todos os documentos a ela fornecidos, inclusive as cópias porventura necessárias, na data estipulada pela Parte Reveladora para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

12. A Parte Recebedora deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da Parte Divulgadora, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

13. A não observância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a Parte infratora, como também o agente causador ou facilitador, por ação ou omissão de qualquer daqueles relacionados neste Termo, ao pagamento, ou recomposição, de todas as perdas e danos, comprovadamente suportados e demonstrados pela outra Parte, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo.

14. As obrigações de confidencialidade decorrentes do presente Termo, tanto quanto as responsabilidades e obrigações outras derivadas do presente Termo, vigorarão durante o período de 5 (cinco) anos após a divulgação de cada Informação Confidencial à Parte Recebedora.

15. O não exercício por qualquer uma das Partes de direitos assegurados neste instrumento não importará em renúncia de tais direitos, sendo tal ato considerado como mera tolerância para todos os efeitos de direito.

16. Alterações do número, natureza e quantidade das Informações Confidenciais disponibilizadas para a Parte Recebedora não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Compromisso de Manutenção de Sigilo, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste Termo.

17. O acréscimo, complementação, substituição ou esclarecimento de qualquer das Informações Confidenciais disponibilizadas para a Parte Recebedora, em razão do presente objetivo, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, não sendo necessário, nessas hipóteses, assinatura ou formalização de Termo Aditivo.

18. Este instrumento não deve ser interpretado como criação ou envolvimento das Partes, ou suas Afiliadas, nem em obrigação de divulgar informações confidenciais para a outra Parte.

19. O fornecimento de Informações Confidenciais pela Parte Divulgadora ou por uma de suas Afiliadas não implica em renúncia, cessão a qualquer título, autorização de uso, alienação ou transferência de nenhum direito, já obtido ou potencial, associado a tais informações, que permanecem como propriedade da Parte Divulgadora ou de suas Afiliadas, para os fins que lhe aprouver.

20. Nenhum direito, licença, direito de exploração de marcas, invenções, direitos autorais, patentes ou direito de propriedade intelectual estão aqui implícitos, incluídos ou concedidos por meio do presente Termo, ou ainda, pela transmissão de Informações Confidenciais entre as Partes.

21. A Contratada declara conhecer todas as Normas, Políticas e Procedimentos de Segurança estabelecidas pela Contratante para execução do Contrato, tanto nas dependências da Contratante como externamente.

22. A Contratada responsabilizar-se-á integralmente e solidariamente, pelos atos de seus empregados praticados nas dependências da Contratante, ou mesmo fora dele, que venham a causar danos ou colocar em risco o patrimônio da Contratante.

23. Este Termo contém o acordo integral entre as Partes com relação ao seu objeto. Quaisquer outros acordos, declarações, garantias anteriores ou contemporâneos com relação à proteção das Informações Confidenciais, verbais ou por escrito, serão substituídos por este Termo. Este Termo será aditado somente firmado pelos representantes autorizados de ambas as Partes.

24. Quaisquer controvérsias em decorrência deste Termo serão solucionadas de modo amistoso através do representante legal das Partes, baseando-se nas leis da República Federativa do Brasil.

E, por estarem assim justas e contratadas, as Partes firmam o presente Instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo indicadas.

_____, _____ de _____ de 20_____

CONTRATADA	**CONTRATANTE**
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx

TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

Ao Conselho Federal de Enfermagem - Cofen

CONTRATO Nº		
OBJETO		
GESTOR DO CONTRATO	**MATRÍCULA**	
CONTRATANTE (ÓRGÃO)		
CONTRATADA	**CNPJ**	
PREPOSTO DA CONTRATADA	**CPF**	

Por este instrumento, os funcionários abaixo-assinado declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes no Conselho Federal de Enfermagem.

_____, _____ de _____ de 20_____

FUNCIONÁRIOS	
<*nome*>	<*nome*>
<*nome*>	<nome>

ANEXO H

MODELO DE TERMO DE COMPARTILHAMENTO DE DADOS E CONFIDENCIALIDADE

O Conselho Federal de Enfermagem (Cofen) visa fomentar os mais altos valores éticos em suas atividades, incluindo quando da escolha de seus parceiros, portanto, faz parte da missão do Cofen "Assegurar à sociedade uma assistência de Enfermagem ética, científica e de qualidade por meio da regulamentação, fiscalização e disciplinamento do exercício profissional".

O Cofen espera que os seus parceiros compartilhem e incorporem os seus valores e o compromisso com a integridade para a construção de um relacionamento duradouro. É seu papel exercer suas atividades dentro dos princípios da ética e dos deveres que a lei impõe, principalmente no que se refere a tomar providências acauteladoras de forma a evitar riscos, incertezas e prejuízos ao Cofen ou terceiros.

Estas cláusulas destinam-se aos "PARCEIROS", os quais abrangem todas as pessoas e empresas que fazem negócios e parcerias, sejam clientes, fornecedores de bens, prestadores de serviços ou estejam envolvidos em qualquer outra espécie de relação contratual com o Conselho Federal de Enfermagem (Cofen).

A aceitação das condições aqui descritas é um pré-requisito para todas as contratações firmadas com o Cofen. Portanto, ao firmar contrato ou criar qualquer parceria com o Cofen, estas disposições serão automaticamente incorporadas como parte do contrato e a CESSIONÁRIA afirma o seu compromisso em cumpri-las.

Quando da execução de suas atividades, Cofen e CESSIONÁRIA compartilharem informações relacionadas a pessoas naturais identificadas ou identificáveis (Dados Pessoais) as Partes serão consideradas como controladoras de tais Dados Pessoais e deverão observar todos os requisitos e limites da Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), bem como as disposições abaixo indicadas. Todos os termos do presente instrumento serão aqueles definidos na LGPD.

1.1. Em qualquer caso, o tratamento dos Dados Pessoais – o que inclui o compartilhamento de tais Dados Pessoais conforme definido pela LGPD – observará a finalidade do contrato. Diante disto, entende-se que Cofen e CESSIONÁRIA apenas realizarão o tratamento de dados estritamente necessários para a realização de sua relação contratual e, em nenhuma hipótese, solicitarão dados de maneira injustificada ou irregular.

1.1.1. O Cofen declara que fornecerá à CESSIONÁRIA acesso a Dados Pessoais apenas na medida em que a CESSIONÁRIA necessite justificadamente, bem como, que previamente a qualquer envio, o Cofen confirmará e/ou providenciará sua autorização legal para fazê-lo.

1.2. Cada Parte será a única responsável por seu tratamento dos Dados Pessoais, incluindo a seleção do método e das finalidades de tratamento, e a determinação da base legal aplicável. Havendo tratamento de dados, o Cofen deverá garantir a existência de uma base de armazenamento válida e segura para o compartilhamento dos Dados Pessoais com a CESSIONÁRIA.

1.3. A CESSIONÁRIA declara e garante ao Cofen que estas declarações e garantias são verdadeiras, precisas, completas e corretas nesta data, e assim permanecerão enquanto a relação com o Cofen permanecer em vigor:

I. Possui um programa adequado e efetivo de conformidade com as leis, regulamentos e quaisquer normativas aplicáveis ao

tratamento de Dados Pessoais, incluindo a LGPD;

II. Dispõe de pessoa para atuar como Encarregado de Dados, nos termos da LGPD, e exceto em caso de hipótese de dispensa válida prevista em lei ou regulamento;

III. Mantém confidenciais os Dados Pessoais e adota políticas e medidas adequadas e efetivas de segurança de informação, compatíveis com a Lei aplicável, com a finalidade do Tratamento dos Dados Pessoais e com os melhores padrões do mercado;

IV. Não realizará qualquer tratamento indevido, irregular ou ilegal, de forma direta e/ou indireta, ativa e/ou passiva, de dados pessoais a que tenha acesso em razão da execução de eventuais contratos celebrados com o Cofen.

V. Tem pleno conhecimento de que todos os Dados Pessoais que forem tratados, durante a vigência da relação entre as Partes, não são passiveis de retenção por período superior ao necessário para o cumprimento das suas obrigações nos termos do(s) contrato(s), ou conforme necessário ou permitido pela lei aplicável.

1.4. A CESSIONÁRIA durante o tratamento de Dados Pessoais e em caso de compartilhamento entre CESSIONÁRIA e Cofen, compromete-se à:

I. Durante o tratamento dos Dados Pessoais, observar e cumprir todas as Leis aplicáveis no momento do tratamento, incluindo a LGPD.

II. Atender, nos termos da LGPD, a toda e qualquer requisição feita pelos titulares de Dados Pessoais, com relação aos Dados Pessoais dos titulares tratados pela CESSIONÁRIA, incluindo, mas não se limitando a: acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; portabilidade dos Dados a outro fornecedor de serviço ou produto, mediante requisição expressa do titular e seguindo regulamentação da Autoridade Nacional de Proteção de Dados (ANPD); eliminação dos dados pessoais tratados com o consentimento do titular exceto nas hipóteses em que a conservação é autorizada conforme previsto na LGPD.

III. Fornecer, mediante solicitação do Cofen, informações completas sobre suas práticas e Política de Tratamento de Dados Pessoais.

IV. Permitir que o Cofen, ou representante devidamente indicado, tenha, mediante solicitação, acesso integral e irrestrito ao ambiente tecnológico da CESSIONÁRIA utilizado em conexão com o tratamento de Dados Pessoais na forma deste contrato, incluindo, mas não se limitando a, qualquer sistema, computador, servidor, máquina virtual, hardware, software ou outro meio ou ferramenta utilizado no tratamento dos Dados Pessoais nas relações contratuais para com o Cofen, desde que isso não interfira em qualquer direito ou obrigação de confidencialidade ou segredo industrial da CESSIONÁRIA.

V. Informar ao Cofen, em até 3 (três) dias úteis do recebimento, se e quando um titular dos Dados Pessoais solicitar pedido de acesso, retificação ou exclusão, ou qualquer outra requisição relacionada aos seus direitos que afete Dados Pessoais tratados pelo Cofen quanto as relações contratuais para com o Cofen.

VI. Não fornecer Dados Pessoais para terceiros, exceto para operadores que realizarão o tratamento em nome de uma das Partes, ou quando permitido pela Lei aplicável.

1.5. O acesso referido no item "IV" da Cláusula 1.4 acima, terá a finalidade de avaliar o cumprimento das obrigações previstas neste documento e a adequação da CESSIONÁRIA ao disposto na Lei aplicável no momento do Tratamento, ficando certo de que a CESSIONÁRIA deverá cooperar com o Cofen ou seu representante no fornecimento de acesso e informações suficientes para atingir tal finalidade, sob pena de arcar com as penalidades por descumprimento contratual estipuladas entre as partes.

1.6. Caso o CESSIONÁRIA tome ciência de qualquer ocorrência, concreta ou suspeita, de perda, mau uso, acesso, destruição, exclusão, comunicação, modificação ou outra forma de tratamento não autorizado dos Dados Pessoais, ou qualquer invasão em sua infraestrutura física ou tecnológica que permita a realização de tais atos, a CESSIONÁRIA informará ao Cofen, por escrito em até 24 horas da ciência do fato, e adotará todas as medidas estabelecidas na Lei aplicável para cessar tal fato.

1.6.1. Tal comunicação deverá indicar, no mínimo a natureza da violação dos dados pessoais, incluindo, sempre que possível, as categorias, o número aproximado de titulares e os respectivos dados violados, a descrição das consequências da violação dos dados pessoais, tanto quanto razoavelmente possível, dadas as circunstâncias, e o plano de contingência tomado pela CESSIONÁRIA para tratar da violação dos dados pessoais e reparar suas consequências.

1.6.2. A CESSIONÁRIA deverá enviar ao Cofen relatórios quinzenais demonstrando o efetivo cumprimento do plano de contingência apresentado.

1.7. A CESSIONÁRIA se obriga a indenizar, defender e manter imune o Cofen, seus conselheiros federais e regionais, diretores, empregados públicos, controladores, Conselhos Regionais de Enfermagem, bem como sucessores e cessionários de

cada um deles (“Partes Indenizáveis”) contra quaisquer perdas e danos, prejuízos, custos, honorários advocatícios (e de outros especialistas, incluindo peritos), depósitos judiciais, penalidades e multas, inclusive no contexto de eventuais reclamações, demandas e processos administrativos, judiciais ou arbitrais contra Partes Indenizáveis movido pelos titulares de Dados Pessoais, pelas Autoridade Governamental, ou por quaisquer terceiros (“Perdas”) que resultarem, direta ou indiretamente, de:

I. qualquer falsidade, omissão, erro, incompletude, violação ou inexatidão nas declarações e garantias prestadas pela CESSIONÁRIA neste documento com relação ao tratamento de Dados Pessoais;

II. inadimplemento de qualquer obrigação com relação ao tratamento de Dados Pessoais prevista neste documento ou estipulado em separado pelas partes, e/ou

II. qualquer ação ou omissão dolosa, culposa ou de má-fé da CESSIONÁRIA que descumpra a Lei aplicável à proteção dos Dados Pessoais.

1.7.1. O direito de indenização pelas Partes Indenizáveis previsto acima em nada estará limitado em razão de:

I. qualquer declaração contida neste documento, Contrato e/ou em seus anexos; e

II. da realização de fiscalização ou auditoria, em especial os direitos previstos na Cláusula 1.4 ou no Contrato.

1.8. A CESSIONÁRIA declara-se ciente, habilitado e preparado a atender, de imediato, aos termos e condições previstas neste instrumento.

1.9. Qualquer violação das obrigações, declarações e garantias estipuladas neste documento será considerada uma violação grave ao contrato, de sorte que o Cofen poderá, a depender da gravidade e a seu exclusivo critério:

I. emitir orientações ou aviso de infração e requerer planos de ação;

II. suspender/paralisar/interditar atividades com justa causa até satisfatória regularização, inclusive, nesta hipótese, com retenção de pagamentos e independentemente do cumprimento do cronograma das atividades em execução;

III. ou rescindir eventuais Contratos de forma motivada, em todos os casos sem prejuízo das penalidades contratuais e eventuais perdas e danos.

1.10. Quaisquer questões, dúvidas, condições de tratamento, incidentes, relacionadas a Dados Pessoais decorrentes da(s) relação(ões) contratual(is) entre as Partes deverão ser prontamente comunicadas entre as partes por seus Encarregados dos Dados, ou Data Protection Officer (DPO).

Brasília, _____ de _____ de 2024.

Nome completo _____

Assinatura _____

Documento assinado eletronicamente por **DAVI LUIZ ANDRADE LOPES VIEIRA - Matr. 320**, **Chefe do Departamento de Tecnologia da Informação e Comunicação**, em 13/11/2024, às 18:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **MATHEUS MOREIRA CRUZ - Matr. 329**, **Integrante Técnico I**, em 13/11/2024, às 19:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **LUIZ GUSTAVO PAULA DE MENEZES JUNIOR - Matr. 568**, **Chefe do Departamento Técnico de Contratações**, em 13/11/2024, às 21:14, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cofen.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0433710** e o código CRC **535E9EBF**.