ANEXO I

TERMO DE REFERÊNCIA

REGISTRO DE PREÇO PARA EVENTUAL CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA FIREWALL, ORQUESTRADOR DE FIREWALL E ENDPOINT, COM PRESTAÇÃO DE SERVIÇOS TÉCNICOS ESPECIALIZADOS EM GESTÃO, CONFIGURAÇÃO E SUPORTE PARA O SESC GOIÁS E SENAC GOIÁS.

1. DEFINIÇÃO DO OBJETO

1.1. Registro de preço para eventual contratação de empresa para fornecimento de solução de segurança firewall, orquestrador de firewall e endpoint, com prestação de serviços técnicos especializados em gestão, configuração e suporte para o Sesc Goiás e Senac Goiás.

2. JUSTIFICATIVA

2.1. DA CONTRATAÇÃO

2.1.1. O Sesc e Senac Goiás tem buscado a modernização e profissionalização dos seus processos internos. Essa modernização passa pelo processo de transformação digital, ou seja, adaptar a cultura institucional a uma nova realidade, adequar recursos humanos e infraestrutura e fazer uso da tecnologia para melhorar o desempenho, ampliar seu alcance e otimizar os resultados;

2.1.2. Os objetivos estratégicos são direcionadores claros e concisos que detalham as mudanças que precisam ser feitas para alcançar a visão de futuro. A estratégia tem como função definir o caminho a ser percorrido para alcançar os objetivos, tirando proveito das forças e oportunidades e mitigando os riscos e fraquezas;

2.1.3. Os objetivos e estratégias de Tecnologia da Informação do Sesc e Senac Regional Goiás representam as "escolhas", baseadas nas melhores alternativas técnicas, que visam a orientar as Instituições quanto as alternativas tecnológicas a serem adotadas e as respectivas decisões sobre investimentos. O quadro a seguir apresenta os objetivos e estratégias da TI para Sesc e Senac Goiás estabelecidos no PDTI:

Objetivos	Estratégias
Prover soluções de TI eficientes e seguras visando atender as	1. Melhoria dos serviços e equipamentos críticos para oferta de conectividade para serviços, funcionários e clientes

necessidades críticas dos funcionários e clientes do Sesc Senac GO	2. Simplificação e maior capacidade de gestão da infraestrutura de datacenter, envolvendo administração regional e unidades
	3. Maior capacidade de oferta de equipamentos para o trabalho, principalmente computadores
	4. Atuação proativa e constante na mitigação dos riscos de segurança
	5. Modernização das soluções tecnológicas para as áreas de negócio por meio de contratações no formato Saas (software as a service)
	6. Reestruturação das plataformas de oferta de serviços digitais aos clientes buscando constituir uma "identidade única" do Sesc Senac GO

2.1.4. A contratação da aquisição, suporte e atualização da solução de firewall é justificada pelos seguintes motivos:

2.1.5. Evolução dos pilares de segurança da informação: Na era da informação, os atributos de segurança da informação, como disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio, são essenciais para proteger a rede de dados contra ameaças cibernéticas. A segurança é um processo contínuo que requer revisão diária de relatórios e acompanhamentos;

2.1.6. Necessidade de proteção contra-ataques cibernéticos: Com a constante evolução dos ataques cibernéticos e divulgação de vulnerabilidades em softwares, é crucial contar com uma solução de firewall robusta para limitar o acesso não autorizado à rede, prevenindo a captura de informações ou prejudicando o funcionamento dos sistemas;

2.1.7. Ampliação da infraestrutura de TI: Com o crescimento da infraestrutura e serviços de Tecnologia da Informação, é imprescindível atualizar e ampliar a solução de proteção de perímetro (firewall) para garantir a segurança de todos os aspectos das ameaças à tecnologia;

2.1.8. Importância da adoção de soluções de segurança: A atualização da solução de firewall é essencial para manter serviços críticos como sites, extranet, correio eletrônico e outros em pleno funcionamento, garantindo a proteção contra ameaças cibernéticas e possíveis consequências graves decorrentes de ataques bem-sucedidos;

2.2. DA ESCOLHA DA MARCA

2.2.1. A Check Point Software Technologies Ltda. é provedora líder de soluções de segurança cibernética para governos e empresas no mundo todo. Suas soluções protegem os clientes contra-ataques cibernéticos de quinta geração com uma taxa líder de captura de malware, ransomware e outros tipos de ataques. A Check Point

oferece arquitetura de segurança de múltiplos níveis, "Infinity" Total Protection com prevenção avançada contra ameaças da Gen V, que defende as informações armazenadas na nuvem, na rede e nos dispositivos móveis das empresas. A Check Point protege mais de 10.000 empresas de todos os tamanhos.

2.2.2. O Sesc e o Senac GO utilizam a solução Check Point a mais de 4 (quatro) anos, que apoia a gestão da segurança da TI nas unidades da área-meio e finalísticas. Ao longo desses anos, foram realizados diversos treinamentos e atividades de mobilização das equipes para uso correto do sistema. Atualmente, do ponto de vista tecnológico, a solução Check Point atende a todos os requisitos funcionais obrigatórios à correta operacionalização das rotinas, considerando as características da infraestrutura de TI das referidas Instituições.

2.2.3. A solução Check Point possui todas as configurações e dados trafegados desde a sua implantação; Tais informações constituem importante acervo para a área de segurança de TI do Sesc e Senac GO. Além disso, foi realizado um considerável investimento na aquisição desta solução e sua manutenção permitirá mantê-la atualizada e em pleno funcionamento durante o período de vigência desta licitação, preservando assim os investimentos já realizados. A aquisição de solução de outro fabricante implicaria no risco de ter duas gerências e soluções que não se conectam entre si, impedindo o gerenciamento centralizado e colocando em risco a segurança do Sesc Goiás e Senac Goiás. Um ataque cibernético bem-sucedido pode ter consequências graves, difíceis de estimar o seu custo para a instituição.

2.2.4. Dessa forma, visando a continuidade, estabilidade e melhoria contínua dos processos administrativos e financeiros do Sesc e Senac Goiás, a manutenção do atual sistema é a solução mais assertiva para o bom andamento dos trabalhos já desenvolvidos. A substituição do sistema, em caso de realização de nova licitação, resultaria em diversos prejuízos operacionais, tais como: necessidade de treinamento para os funcionários, a excessiva demanda de tempo e recursos da equipe da tecnologia da informática para migrar todas os dados de um sistema para outro além do risco de perda de dados indispensáveis para atender as exigências deste processo.

2.2.5. A opção pela continuidade dos produtos Check Point Software Technologies mantém a padronização do ambiente do Sesc e Senac Goiás. De fato, há precedentes na jurisprudência que apontam para a possibilidade de se observar o princípio da padronização, sem conflitar com a vedação da preferência de marca, a exemplo do Acórdão-TCU nº 1521/2003, do Plenário, o qual pondera que a indicação de marca na especificação de produtos de informática pode ser aceita frente ao princípio da padronização, desde que a decisão administrativa que venha a identificar o produto pela sua marca seja circunstanciadamente motivada em termos técnicos e econômicos, mais vantajosa para a administração.

2.2.6. Sendo assim, concluímos que somente a marca Check Point Software Technologies é a ESCOLHIDA, conforme defendido neste documento.

3. JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇOS, CONTRATAÇÃO POR LOTE ÚNICO E DA POSSIBILIDADE DE SUBCONTRATAÇÃO

3.1. O objeto do presente processo trata-se de quantidade meramente estimativa, a ser demandada de acordo com a necessidade da Instituição, devendo ser processada pelo Sistema de Registro de Preço, tendo em vista que são aquisições nas quais não é possível definir antecipadamente, e com precisão, a quantidade necessária dos itens descritos para atender a demanda do Sesc e Senac Goiás.

3.2. Assim, podendo haver a variação da demanda, a quantidade descrita no **QUADRO DESCRITIVO E QUANTITATIVO SESC E SENAC,** refere-se a mera estimativa, sem previsão exata de quantos produtos/serviços de fato serão adquiridos/ executados.

3.3. Desse modo, a escolha pela utilização do Sistema de Registro de Preços nesta contratação justifica-se com base no Regulamento de Licitações e Contratos do Sesc (Resolução n.º 1.252/2012) e Regulamento de Licitações e Contratos do Senac (Resolução n.º 958/2012), que, em seu artigo 33, prevê as hipóteses de utilização do referido sistema, quais sejam:

> ***Art. 33.*** *O registro de preço, sempre precedido de concorrência ou de pregão, poderá ser utilizado nas seguintes hipóteses:*
> ***I - quando for mais conveniente que a aquisição demande entrega ou fornecimento parcelado;***
> *II - quando, pelas características do bem ou do serviço, houver necessidade de aquisições frequentes;*
> ***III - quando não for possível estabelecer, previamente, o quantitativo exato para o atendimento das necessidades****.*
> *(Grifou-se)*

3.4. Assim, a escolha pelo Sistema de Registro de Preços torna-se vantajosa para o Sesc e Senac Goiás porque não fica obrigado a adquirir o quantitativo máximo de produtos e nem à contratação e execução total dos serviços, e de forma imediata, visto que a quantidade prevista no contrato e/ou instrumento equivalente é estimada e, portanto, a prestação do serviço e entrega dos produtos se dará de acordo com a demanda do Sesc e Senac Goiás.

3.5. Da mesma forma, a utilização do Sistema de Registro de Preços nesta contratação decorre do fato da escalabilidade da solução, proporcionando a contratação mais adequada de acordo com a necessidade de expansão do ambiente em dizeres de volumetria e processamento, como também possibilitando entregas de serviços com novas arquiteturas, devendo a contratação operar sob demanda, o que configura a natureza da contratação por registro de preços.

3.6. Assim sendo, estamos diante de uma estimativa do que é possível o Sesc e o Senac Goiás se utilizar durante o período de 12 meses. Porém, por se tratar de

demanda futura, se faz necessário o registro de preços destes produtos e serviços para assegurar a economicidade ao Sesc e Senac Goiás, devendo estas demandas serem executadas em tempo oportuno, conforme a necessidade, consoante o disposto no artigo 33, da Resolução n.º 1.252/2012 do Sesc e da Resolução nº 958/2012 do Senac, citado acima, bem como no artigo 3º, do Decreto 7.892/2013, que Regulamenta o Sistema de Registro de Preços na esfera Federal, prevendo o seguinte:

> *Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:*
> *I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;*
> *II - **quando for conveniente a aquisição de bens com previsão de entregas parceladas** ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
> *III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou*
> *IV - **quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.***

3.7. Além disso, o Tribunal de Contas da União, atento às vantagens oferecidas pelo Sistema de Registro de Preços, tem recomendado sua adoção, inclusive para evitar o fracionamento de despesa, vejamos:

> *[...] j.2) **com o intuito de evitar o fracionamento de despesa, vedado pelo art. 23, § 2º, da Lei n.º 8.666/93, utilizar-se, na aquisição de bens, do sistema de registro de preços de que tratam o inciso II. e §§ 1º e 4º, do art. 15, da citada Lei, regulamentado pelo Decreto nº 2.743, de 21.8.1998;** (Decisão nº 472/1999, Plenário, Rel. Min. Valmir Campelo, Processo TC 675.048.1998-2);*
>
> *[...] 3.1.7. Quanto à diminuta disponibilidade orçamentária e financeira da UG 153076, bem como quanto à liberação fracionada dos créditos orçamentários, temos que o gestor poderia contornar essas dificuldades com um planejamento eficiente. Ademais, **o Sistema de Registro de Preços, previsto no art. 15 da Lei nº 8.666/93 e regulamentado pelo Decreto nº 2.743, de 21 de agosto de 1998, presta-se bem às dificuldades apresentadas pelos responsáveis.** (Acórdão nº 3.146/2004, Primeira Câmara, Rel. Min. Guilherme Palmeira Processo TC 009.989/2003-1).*

3.8. De igual modo, a jurisprudência do TCU corrobora:

[...] 4. Com relação à utilização do registro de preços para a licitação, o órgão a justificou com base na mudança no modelo de gestão de impressão ora em curso, de um sistema de aquisição dos bens necessários, com os custos associados à obsolescência e manutenção, para um sistema de contratação desses serviços. Em vista das restrições orçamentárias, o sistema de registro de preços permitiria a implantação gradativa dos serviços. ***A solução adotada se amolda ao previsto no art. 3º, inciso II, do Decreto nº 7.892/2013, a saber: "Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses: (...) II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;" 5. No mesmo sentido os Acórdãos nºs 1.737/2012 e 3.092/2014, ambos do Plenário. Desse modo, a justificativa pode ser acolhida****. (TCU, Processo 011.393/2016-5, Acórdão 2438/2016 - Plenário, Relator: JOSÉ MUCIO MONTEIRO, data da sessão: 21/09/2016);*

[...] 3. A utilização do Sistema de Registro de Preços é possível, nos termos do art. 3º, inciso II, do Decreto 7.892/2013, quando for conveniente a aquisição de bens com previsão de entregas parceladas. Não há que se confundir, todavia, entrega parcelada com entrega de parcelas do produto. A primeira ocorre quando são demandadas várias aquisições do objeto licitado na configuração em que prevista pelo órgão responsável pelo Sistema de Registro de Preços. A segunda, que não é albergada pela legislação retro mencionada, cuida de aquisições em que são demandadas partes do objeto licitado em quantitativos diferentes daqueles inicialmente previstos. *4. A impossibilidade de aquisição separada de itens de objeto adjudicado por preço global em contratações realizadas por meio de Sistema de Registro de Preços foi ratificada pelo TCU mediante o subitem 9.3.2 do Acórdão 757/2015 - Plenário. 5. O mencionado subitem 9.3.2 daquele decisum confirmou, ainda, a tese de que, no Sistema de Registro de Preços, a adjudicação por item é a regra geral, sendo a opção pelo lote único excepcional, devendo ser plenamente motivada. 6. Nos termos do Enunciado 258 da Súmula de jurisprudência do TCU, as composições de custos unitários e o detalhamento de encargos sociais e do BDI integram o orçamento que compõe o projeto básico da obra ou serviço de engenharia, devem constar dos anexos do edital de licitação e das propostas das licitantes e não podem ser indicados mediante uso da expressão verba ou de unidades genéricas. (TCU 01917720143, Relator: MARCOS BEMQUERER, Data de Julgamento: 27/01/2016). (Grifou-se)*

3.9. Dessa feita, a licitação mostra-se mais vantajosa para o Sesc e Senac Goiás se processada pelo Sistema de Registro de Preço e pelo critério de julgamento menor valor por lote, com base nas recomendações proferidas pelo Tribunal de Contas da União, sendo algumas citadas acima, bem como em representação assim julgada: "*...A utilização do Sistema de Registro de Preços é adequada em situações em que a demanda é incerta, seja em relação a sua ocorrência, seja no que concerne à quantidade de bens a ser demandada.*" (Acórdão 2197/2015-Plenário. GRUPO I – CLASSE VII – Plenário TC nº 028.924/2014-2. Natureza: Representação. Órgão: Ministério da Integração Nacional. Relator: Benjamin Zymler. Data da sessão: 02/09/2015).

3.10. Ante o exposto, a contratação por meio do Sistema de Registro de Preços, no presente caso, é uma forma de economia para o Sesc e Senac Goiás, tendo em vista que acarreta menos licitações, mais rapidez nas aquisições dos itens descritos e ainda elimina eventual problema de armazenamento dos produtos.

3.11. Ante o exposto, justifica-se que a utilização do registro de preços nesta contratação possui previsão legal, está em conformidade com o disposto no Regulamento de Licitações e Contratos do Sesc e do Senac e com o entendimento do Tribunal de Contas da União, e ainda é a opção que possibilita a busca da economicidade para o Sesc e Senac Goiás, além da prestação de um serviço de qualidade e por um único fornecedor apto a lidar com a marca dos objetos adquiridos.

3.12. O Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação, elaborado pelo TCU[1], discorre de maneira extensa sobre o assunto, estabelecendo a seguinte definição: "Uma solução de TI engloba todos os elementos necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou. Como foi exposto no item "2.1. Conceito de solução de TI" do Guia, uma solução de TI normalmente engloba mais elementos do que, por exemplo, somente o desenvolvimento de um sistema, a contratação de licenças de um software ou a contratação de um equipamento."

3.13. O não-parcelamento deste processo licitatório justifica-se pela necessidade da interoperabilidade e não divisão da solução como todo. É fundamental assegurar que todos os equipamentos e subscrições descritas neste edital, sejam ofertados de um mesmo fabricante, garantindo que as partes estejam estritamente alinhadas em termos de versões, funcionalidades e compatibilidade. A eventual divisão com fracassos de itens do ora lote poderia inviabilizar a aquisição da solução pretendida, dado que composta de vários elementos e características da solução que trazem vantajosidade na aquisição de um único fabricante e por fim, lote único.

3.14. Além do supramencionado, no modelo de atendimento adotado, a não-separação em itens distintos se deu devido à necessidade de ser uma solução completamente integrada que possa tratar as especificidades de cada um dos itens de acordo com as suas métricas, acordos de nível de serviço, especialização de

[1] Guia de boas práticas em contratação de soluções de tecnologia da informação (TCU, 2012)

equipes de profissionais, regime de atendimento, além da específica contribuição de cada item para o resultado final da contratação. Neste sentido, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do contrato.

3.15. Conforme extraído do site da Zênite[2], a subcontratação ocorre quando o particular contratado pela Administração transfere a execução de partes do objeto terceiro por ele contratado e que não mantém vínculo contratual com a Administração. Trata-se, portanto, de uma relação jurídica de natureza civil, própria e autônoma em relação àquela firmada com a Administração, a qual vincula apenas o contratado e o subcontratado, cabendo, contudo, à Administração Contratante autorizar sua formação no caso concreto, quando admitida nos instrumentos convocatório e contratual.

3.4. O projeto deverá ser implementado de forma a garantir a compatibilidade de acesso às informações tratadas por ela em relação às políticas de segurança do Sesc e do Senac Goiás, podendo ser admitida a subcontratação de partes do objeto contratual até o limite de 30%, desde que mantida a responsabilidade do Contratado perante o Contratante, sendo vedada a subcontratação com licitante que tenha participado do procedimento licitatório, nos termos do Regulamento de Licitações e Contratos do Sesc e do Senac Goiás.

4. ESPECIFICAÇÕES TÉCNICAS

4.1. QUADRO DESCRITIVO E QUANTITATIVO SESC E SENAC

LOTE 01 (ÚNICO)				
Inst.	**Itens**	**Descrição**	**Unidade de Medida**	**Qnt.**
SESC	1	ORQUESTRADOR DE FIREWALL	Unid.	1
	2	FIREWALL TIPO I	Unid.	1
	3	FIREWALL TIPO III	Unid.	7
	4	FIREWALL TIPO IV	Unid.	3
	5	SUBSCRIÇÃO FIREWALL TIPO I	Serv.	1
	6	SUBSCRIÇÃO FIREWALL TIPO III	Serv.	7
	7	SUBSCRIÇÃO FIREWALL TIPO IV	Serv.	3
	8	SUBSCRIÇÃO DE ENDPOINT	Serv.	1600
	9	SERVIÇO GERÊNCIA E SUPORTE ESPECIALIZADO	Mês	12
SENAC	10	ORQUESTRADOR DE FIREWALL	Unid.	1
	11	FIREWALL TIPO I	Unid.	1
	12	FIREWALL TIPO II	Unid.	1
	13	FIREWALL TIPO III	Unid.	12
	14	FIREWALL TIPO IV	Unid.	8
	15	SUBSCRIÇÃO GERENCIAMENTO CENTRALIZADO	Serv.	1

Extraído de: [2] https://zenite.blog.br/sendo-possivel-a-subcontratacao-de-parcela-do-objeto-deve-se-exigir-documentos-de-habilitacao-do-subcontratado-tais-documentos-serao-os-mesmos-exigidos-dos-participantes-da-licitacao/ em 06 de junho de 2023.

	16	SUBSCRIÇÃO FIREWALL TIPO I	Serv.	1
	17	SUBSCRIÇÃO FIREWALL TIPO II	Serv.	1
	18	SUBSCRIÇÃO FIREWALL TIPO III	Serv.	12
	19	SUBSCRIÇÃO FIREWALL TIPO IV	Serv.	8
	20	SUBSCRIÇÃO DE ENDPOINT	Serv.	2000
	21	SERVIÇO GERÊNCIA E SUPORTE ESPECIALIZADO	Mês	12

4.2. CARACTERÍSTICAS GERAIS DOS EQUIPAMENTOS DE FIREWALL TIPO I, TIPO II, TIPO III E TIPO IV

4.2.1. CARACTERÍSTICAS GERAIS

4.2.1.1. Solução completa de proteção de rede do tipo Firewall de Próxima Geração (Next Generation Firewall – NGFW), para segurança de perímetro que inclui filtro de pacote, controle de aplicação (App Control), administração de largura de banda (QoS), VPN IPSec e SSL, Sistema de Prevenção de Intrusão (IPS), prevenção contra ameaças de vírus (Antivírus), spywares e malwares "Zero Day", Filtro de URL (CFS), bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança integrada e robusta;

4.2.1.2. A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

4.2.1.3. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

4.2.1.4. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

4.2.1.5. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

4.2.1.6. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

4.2.1.7. Equipamento Orquestrador de Firewall devem ser próprios para montagem em rack "19" e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

4.2.1.8. Equipamento Firewall Tipo I, Tipo II e Tipo III devem ser próprios para montagem em rack "19" e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

4.2.1.9. A solução de Firewall deverá consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e consoles de gerência e de monitoração;

4.2.1.10. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos, apresentada com uma planilha ponto a ponto, junto a proposta comercial, que comprove o atendimento dos requisitos, indicando a página da documentação técnica onde consta o requisito.

4.2.1.11. Caso não seja o fabricante da solução, a licitante deverá apresentar declaração do fabricante da solução ofertada, dirigida a contratante, junto a proposta

comercial, informando que é revenda autorizada no Brasil, estando apta a comercializar, prestar suporte e garantia dos produtos e serviços ofertados;

4.2.2. **FUNCIONALIDADES DE FIREWALL**

4.2.2.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de proteção de próxima geração;

4.2.2.2. 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 técnica;

4.2.2.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

4.2.2.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

4.2.2.5. Realizar upgrade via SCP, SFTP e https via interface WEB

4.2.2.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

4.2.2.7. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

4.2.2.8. Deverá suportar VXLAN;

4.2.2.9. Deve suportar os seguintes tipos de NAT:

4.2.2.10. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

4.2.2.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.2.2.12. As regras de NAT devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;

4.2.2.13. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

4.2.2.14. Enviar logs para sistemas de monitoração externos, simultaneamente;

4.2.2.15. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

4.2.2.16. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall;

4.2.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.2.2.18. Suportar OSPF graceful restart;
4.2.2.19. Deve suportar roteamento ECMP (equal cost multi-path);
4.2.2.20. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultanea usando os seguintes parametros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;
4.2.2.21. Autenticação integrada via Kerberos;
4.2.2.22. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP;
4.2.2.23. As regras Firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;
4.2.2.24. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;
4.2.2.25. A solução deve ter a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);
4.2.2.26. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;
4.2.2.27. Deve possuir mecanismo de ativação de validada da regra com período customizado;
4.2.2.28. Deverá suportar redundância e balancemento de links, tendo capacidade a no mínimo 3 links de internet;
4.2.2.29. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento;
4.2.2.30. Deve permitir a configuração do tempo de checagem para cada um dos links;

4.2.3. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**
4.2.3.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
4.2.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.2.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3;
4.2.3.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.2.3.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

4.2.3.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

4.2.3.6.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

4.2.3.6.2. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.2.3.7. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.2.3.8. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

4.2.3.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.2.3.10. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

4.2.3.11. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.2.3.12. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

4.2.3.13. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

4.2.3.14. Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação princial e/ou as suas sub-categorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como "Facebook" ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de applicações WEB que a propria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

4.2.3.15. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.2.3.16. Atualizar a base de assinaturas de aplicações automaticamente;

4.2.3.17. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.2.3.18. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

4.2.3.19. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.2.3.20. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

4.2.3.21. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.2.3.22. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.2.3.22.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.2.3.22.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.2.3.22.3. Deverá 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 Active Directory e base de dados local;

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

4.2.3.22.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

4.2.3.22.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

4.2.3.22.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

4.2.3.22.8. Suportar a criação de categorias de URLs customizadas;

4.2.3.22.9. Suportar a exclusão de URLs do bloqueio, por categoria;

4.2.3.22.10. Permitir a customização de página de bloqueio;

4.2.3.23. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.2.3.24. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

4.2.3.25. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

4.2.4. **FUNCIONALIDADE DE FILTRO DE DADOS**

4.2.4.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

4.2.4.1.1. PCI - credit card numbers;
4.2.4.1.2. HIPAA - Medical Records Number – MRN;
4.2.4.1.3. International Bank Account Numbers – IBAN;
4.2.4.1.4. Source Code – JAVA;
4.2.4.1.5. U.S. Social Security Numbers - According to SSA;
4.2.4.1.6. Salary Survey Terms;
4.2.4.1.7. Viewer File – PDF;
4.2.4.1.8. Executable file;
4.2.4.1.9. Database file;
4.2.4.1.10. Document file;
4.2.4.1.11. Presentation file;
4.2.4.1.12. Spreadsheet file;

4.2.4.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

4.2.4.3. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

4.2.4.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS;

4.2.5. **FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS**

4.2.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

4.2.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

4.2.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

4.2.5.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.2.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;
4.2.5.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.2.5.7. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
4.2.5.8. Detectar e bloquear a origem de portscans;
4.2.5.9. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.2.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.2.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.2.5.12. Suportar bloqueio de arquivos por tipo;
4.2.5.13. Identificar e bloquear comunicação com botnets;
4.2.5.14. Deve suportar referência cruzada com CVE;
4.2.5.15. Em cada proteção de segurança, deve estar incluso informações como:
4.2.5.15.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;
4.2.5.15.2. Severidade;
4.2.5.15.3. Tipo de ação a ser executada.
4.2.5.16. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.
4.2.5.17. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.
4.2.5.18. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.
4.2.5.19. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)
4.2.5.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.2.5.21. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.2.5.22. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.2.5.23. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;
4.2.5.24. A solução de IPS, deve possuir mecanismo de analise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

4.2.5.25. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;
4.2.5.26. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;
4.2.5.27. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.
4.2.5.28. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;
4.2.5.29. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;
4.2.5.30. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;
4.2.5.31. A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;
4.2.5.32. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.
4.2.5.33. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso
4.2.5.34. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;
4.2.5.35. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;
4.2.5.36. A solução deve permitir a criação de White list baseado no MD5 do arquivo;
4.2.5.37. Os eventos devem identificar o país de onde partiu a ameaça;
4.2.5.38. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;
4.2.5.39. Suportar rastreamento de vírus em arquivos pdf;
4.2.5.40. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.2.5.41. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.2.5.42. Em caso de falha no mecanismo de inspeção do Anti-Virus, deve ser possível configurar se as conexões serão permitidas ou bloqueada
4.2.5.43. A solução de Anti-virus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a

interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

4.2.5.44. A solução Antivirus deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

4.2.5.45. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

4.2.5.46. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.2.5.47. A solução deverá possuir mecanismo de "machine learning" para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorith) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

4.2.5.48. A solução deverá possuir mecanismo de "machine learning" para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

4.2.5.49. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

4.2.5.50. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

4.2.5.51. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

4.2.5.52. A solução Antivírus deverá suportar a análise de links no corpo de e-mails;

4.2.6. **FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO**

4.2.6.1. Suportar a criação de políticas de QoS por:

4.2.6.2. Endereço de origem, endereço de destino e por porta;

4.2.6.3. O QoS deve possibilitar a definição de classes por:

4.2.6.4. Banda garantida, banda máxima e fila de prioridade;

4.2.6.5. Disponibilizar estatísticas em tempo real para classes de QoS;

4.2.7. **FUNCIONALIDADES DE VPN**

4.2.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

4.2.7.2. Suportar IPSec VPN;

4.2.7.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

4.2.7.4. Suportar SSL VPN;

4.2.7.5. A VPN IPSEc deve suportar:

4.2.7.6. 3DES, Autenticação MD5, SHA-1, SHA-384, AES-XCBC, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

4.2.7.7. A VPN SSL deve suportar:

4.2.7.8. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.2.7.9. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.2.7.10. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

4.2.7.11. Atribuição de endereço IP nos clientes remotos de VPN;

4.2.7.12. Atribuição de DNS nos clientes remotos de VPN;

4.2.7.13. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

4.2.7.14. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

4.2.7.15. A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.

4.2.7.16. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

4.2.7.17. A solução deve permitir a integração da ferramenta com provedores de identidade, através de SAML, para autenticação dos usuários remotos conectados via VPN;

4.2.7.18. Suportar leitura e verificação de CRL (certificate revocation list);'

4.2.7.19. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

4.2.7.20. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

4.2.8. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

4.2.8.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

4.2.8.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

4.2.8.3. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

4.2.8.4. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

4.2.8.5. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA

durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

4.2.8.6. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

4.2.8.7. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

4.2.8.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

4.2.8.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

4.2.8.10. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

4.2.8.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

4.2.8.12. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

4.2.8.13. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

4.2.8.14. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

4.2.8.15. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

4.2.8.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

4.2.8.17. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

4.2.8.18. A solução deve suportar inspeção para o protocolo SMBv3;

4.2.8.19. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

4.2.8.20. A solução deve possuir engine de inspeção a nível de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

4.2.8.21. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a

necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

4.2.8.22. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede e endereço IP;

4.2.8.23. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

4.2.8.24. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

4.2.8.25. Possibilitar remoção de conteúdo ativo dinamicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

4.2.8.26. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

4.2.8.27. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

4.2.8.28. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

4.2.8.29. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

4.2.8.30. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

4.2.8.31. Número de arquivos emulados;

4.2.8.32. Número de arquivos com malware.

4.2.8.33. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

4.2.8.34. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

4.2.8.35. O tamanho máximo do arquivo emulado seja excedido;

4.2.8.36. O tempo máximo de emulação seja excedido;

4.2.9. **SD-WAN**

4.2.9.1. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE (Private or Public APN) e Satélite;

4.2.9.2. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup;

4.2.9.3. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real;

4.2.9.4. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

4.2.9.5. Deve permitir a comunicação indireta entre localidades por meio de uma topologia "hub and spoke";

4.2.9.6. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

4.2.9.7. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

4.2.9.8. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay;

4.2.9.9. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

4.2.9.10. Suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional;

4.2.9.11. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

4.2.9.12. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

4.2.9.13. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem;

4.2.9.14. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala;

4.2.9.15. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional;

4.2.9.16. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes;

4.2.9.17. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade;

4.2.9.18. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar;

4.2.9.19. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo);

4.2.9.20. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente;
4.2.9.21. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos;
4.2.9.22. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional;
4.2.9.23. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN;
4.2.9.24. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade;
4.2.9.25. Realizar medições de "Latência"/"Jitter"/"Queda de pacotes" em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção;

4.3. ITEMS 1 E 10 –ORQUESTRADOR DE FIREWALL

4.3.1. Maestro Hyperscale Orchestrator 140
4.3.1.1. A solução de a que se refere este item terá por finalidade prover o balanceamento entre os appliances de Next generation Firewall, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades;
4.3.1.2. A solução de balanceamento deve permitir que a solução de NG Firewall se torne escalável;
4.3.1.3. A solução deve suportar a orquestração entre appliances de modelos diferentes, do mesmo fabricante, de modo a prover a escalabilidade ao longo do tempo;
4.3.1.4. A solução de balanceamento deverá ser fornecida em appliances físicos;
4.3.1.5. A solução de balanceamento deverá ser fornecida em alta disponibilidade do tipo Ativo/Ativo;
4.3.1.6. Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência;
4.3.1.7. A solução deverá ser provida de forma redundante, de modo que se houver a falha de uma delas, a outra possa assumir totalmente o controle, sem que haja perda do tráfego;
4.3.1.8. A solução deve ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;
4.3.1.9. Cada Grupo de Segurança deverá comportar, no mínimo, 8 (oito) appliances;
4.3.1.10. A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;
4.3.1.11. A solução deverá ser capaz de conectar, no mínimo, 24 (vinte e quatro) appliances Next Generarion Firewall a 10 Gbps com interfaces 10GBase-SR do tipo SFP+ e 4 Appliances a 100 Gbps de forma redundante;

4.3.1.12. A solução deverá possuir no mínimo 02 (duas) interfaces de rede 10/100/1000BaseT com portas de cobre, do tipo UTP (RJ-45);
4.3.1.13. A solução de balanceamento deverá ser acompanhada de, no mínimo 8 (oito) transceptores para conectar os appliances NGFirewall;
4.3.1.14. A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência;
4.3.1.15. A solução de balanceamento deverá suportar, no mínimo 250 Gbps de throughput;
4.3.1.16. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos, apresentada com uma planilha ponto a ponto, junto a proposta comercial, que comprove o atendimento dos requisitos, indicando a página da documentação técnica onde consta o requisito;
4.3.1.17. Caso não seja o fabricante da solução, a licitante deverá apresentar declaração do fabricante da solução ofertada, dirigida a contratante, junto a proposta comercial, informando que é revenda autorizada no Brasil, estando apta a comercializar, prestar suporte e garantia dos produtos e serviços ofertados;
4.3.1.18. O equipamento deverá ser ofertado com garantia do fabricante por 60 meses;

4.4.ITENS 2 E 11 –FIREWALL TIPO I

4.4.1. Quantum 7000 Security Gateway
4.4.1.1. Fica a critério do fornecedor, inserir todos os componentes necessários para que o item seja entregue com todas as características solicitadas;
4.4.1.2. Threat Prevention 9.5 Gbps;
4.4.1.3. NGFW Throughput 22 Gbps;
4.4.1.4. IPS Throughput 25 Gbps;
4.4.1.5. Firewall 48 Gbps;
4.4.1.6. Concurrent Connections 16M;
4.4.1.7. 1 x CPUs, 16 Physical Cores, 32 Virtual Cores;
4.4.1.8. 2 x 480 GB SSD Storage;
4.4.1.9. 2 x AC PSU;
4.4.1.10. 64 GB Memory RAM;
4.4.1.11. 8 x 1 GbE Ports;
4.4.1.12. 1 x 1 GbE Port Sync;
4.4.1.13. 1 x 1 GbE Port Management;
4.4.1.14. 8 x 10 GbE SFP+ Port;
4.4.1.15. 8 x Cabos 10G SFP+ DAC 3 metros;
4.4.1.16. O equipamento deverá ser ofertado com garantia do fabricante por 60 meses;

4.5.ITEM 12 – FIREWALL TIPO II

4.5.1. Quantum 6200 Security Gateway

4.5.1.1. Fica a critério do fornecedor, inserir todos os componentes necessários para que o item seja entregue com todas as características solicitadas;
4.5.1.2. Threat Prevention 1.8 Gbps;
4.5.1.3. NGFW 3.72 Gbps;
4.5.1.4. IPS 4.65 Gbps;
4.5.1.5. Firewall 9 Gbps;
4.5.1.6. Concurrent Connections 8M;
4.5.1.7. 1 x CPUs, 2 Physical Cores, 4 Virtual Cores;
4.5.1.8. 1 x 240 GB SSD Storage;
4.5.1.9. 2 x AC PSU;
4.5.1.10. 32 GB Memory RAM;
4.5.1.11. 8 x 1 GbE Port;
4.5.1.12. 4 x 10 GbE SFP+ Port;
4.5.1.13. 1 x 1 GbE Port Management;
4.5.1.14. 1 x 1 GbE Port Sync;
4.5.1.15. 4 x Cabos 10G SFP+ DAC 3 metros;
4.5.1.16. O equipamento deverá ser ofertado com garantia do fabricante por 60 meses;

4.6. ITENS 3 E 13 –FIREWALL TIPO III

4.6.1. Quantum 1600 Security Gateway
4.6.1.1. Fica a critério do fornecedor, inserir todos os componentes necessários para que o item seja entregue com todas as características solicitadas;
4.6.1.2. Threat Prevention 1.5 Gbps;
4.6.1.3. NGFW 3.2 Gbps;
4.6.1.4. IPS 3.5 Gbps;
4.6.1.5. Firewall 4.8 Gbps;
4.6.1.6. Concurrent Connections 2.4M;
4.6.1.7. Micro-SD card slot 64;
4.6.1.8. eMMC 32 GB;
4.6.1.9. 16 x 1 GbE LAN Port;
4.6.1.10. 1 x 1 GbE DMZ Port;
4.6.1.11. 1 x 1 GbE WAN Port
4.6.1.12. O equipamento deverá ser ofertado com garantia do fabricante por 60 meses;

4.7. ITENS 4 E 14 –FIREWALL TIPO IV

4.7.1. Quantum 3600 Security Gateway
4.7.1.1. Fica a critério do fornecedor, inserir todos os componentes necessários para que o item seja entregue com todas as características solicitadas;
4.7.1.2. Threat Prevention 780 Mbps;
4.7.1.3. NGFW 1.5 Gbps;
4.7.1.4. IPS 1.99 Gbps;

4.7.1.5. Firewall 3.3 Gbps;
4.7.1.6. Concurrent Connections 2M;
4.7.1.7. 1 x CPUs, 4 Physical Cores;
4.7.1.8. 1 x 240 GB SSD storage;
4.7.1.9. 8 GB RAM;
4.7.1.10. 5 x 1 GbE Port;
4.7.1.11. 1 x 1 GbE Port Management;
4.7.1.12. O equipamento deverá ser ofertado com garantia do fabricante por 60 meses;

4.8. ITEM 15 – SUBSCRIÇÃO GERENCIAMENTO CENTRALIZADO

4.8.1.1. Next Generation Security Management Software para 50 gateways;
4.8.1.2. SmartEvent;
4.8.1.3. Compliance;
4.8.1.4. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada;
4.8.1.5. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;
4.8.1.6. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;
4.8.1.7. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;
4.8.1.8. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;
4.8.1.9. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;
4.8.1.10. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
4.8.1.11. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;
4.8.1.12. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);
4.8.1.13. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.
4.8.1.14. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
4.8.1.15. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.8.1.16. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;
4.8.1.17. Suportar backup das configurações e rollback de configuração para a última configuração salva;
4.8.1.18. Suportar validação de regras antes da aplicação;
4.8.1.19. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
4.8.1.20. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;
4.8.1.21. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
4.8.1.22. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
4.8.1.23. Permitir a criação de certificados digitais para autenticação de usuários;
4.8.1.24. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);
4.8.1.25. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.
4.8.1.26. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;
4.8.1.27. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.
4.8.1.28. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.
4.8.1.29. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.
4.8.1.30. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;
4.8.1.31. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;
4.8.1.32. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;
4.8.1.33. Deve ser possível exportar os logs em CSV ou TXT;
4.8.1.34. A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;
4.8.1.35. A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

4.8.1.36. A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

4.8.1.37. O visualizador de log deve ter um recurso de pesquisa de texto livre;

4.8.1.38. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

4.8.1.39. Possibilitar rotação do log;

4.8.1.40. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

4.8.1.41. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

4.8.1.42. Deve permitir a criação de relatórios personalizados;

4.8.1.43. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

4.8.1.44. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI);

4.8.1.45. Possui capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

4.8.1.46. Deve consolidar logs e relatórios de todos os dispositivos administrados;

4.8.1.47. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.8.1.48. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

4.8.1.49. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

4.8.1.50. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo.

4.8.1.51. ISO 27001 e ISO 27002;

4.8.1.52. PCI-DSS;

4.8.1.53. NIST 800-41;

4.8.1.54. GDPR (base da norma LGPD);

4.8.1.55. Não sendo permitido licenciamento mensalizado "trial", ou seja, deve ser considerado uma licença de uso durante o período da garantia.

4.8.1.56. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas "Software Livre".

4.8.1.57. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

4.8.1.58. Permitir a customização do padrão regulatório da própria instituição;

4.8.1.59. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

4.8.1.60. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

4.8.1.61. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;

4.8.1.62. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

4.8.1.63. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

4.8.1.64. Possuir alertas de políticas e potenciais violações de conformidade;

4.8.1.65. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

4.8.1.66. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

4.8.1.67. Permitir que os relatórios possam ser salvos, enviados e impressos;

4.8.1.68. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino;

4.8.1.69. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

4.8.1.70. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

4.8.1.71. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

4.8.1.72. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

4.8.1.73. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.8.1.74. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

4.8.1.75. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

4.8.1.76. Criar certificados digitais para acesso dos usuários VPN;

4.8.1.77. Criar certificados digitais para VPNs Site-to-Site;

4.8.1.78. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

4.8.1.79. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

4.8.1.80. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

4.8.1.81. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

4.8.1.82. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

4.8.1.83. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa.

4.8.1.84. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

4.8.1.85. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

4.8.1.86. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

4.8.1.87. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

4.8.1.88. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

4.8.1.89. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

4.8.1.90. A solução deve ser capaz de personalizar e criar regras de correlação;

4.8.1.91. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

4.8.1.92. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

4.8.1.93. Caso não seja o fabricante da solução, a licitante deverá apresentar declaração do fabricante da solução ofertada, dirigida a contratante, junto a proposta comercial, informando que é revenda autorizada no Brasil, estando apta a comercializar, prestar suporte e garantia dos produtos e serviços ofertados;

4.9. ITENS 5 E 16 – SUBSCRIÇÃO FIREWALL TIPO I

4.9.1. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada:

4.9.1.1. Firewall;
4.9.1.2. VPN (IPsec);
4.9.1.3. Mobile Access;
4.9.1.4. Identity Awareness;
4.9.1.5. Application Control;
4.9.1.6. Content Awareness;
4.9.1.7. IPS;
4.9.1.8. URL Filtering;
4.9.1.9. Anti-Bot;
4.9.1.10. Anti-Virus;
4.9.1.11. Anti-Spam;
4.9.1.12. DNS Security;
4.9.1.13. SandBlast Threat Emulation;
4.9.1.14. SandBast Threat Extraction;
4.9.1.15. Zero-phishing;
4.9.1.16. SD-WAN;

4.10. ITEM 17 – SUBSCRIÇÃO FIREWALL TIPO II PARA 5 ANOS

4.10.1. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada:

4.10.1.1. Firewall;
4.10.1.2. VPN (IPsec);
4.10.1.3. Mobile Access;
4.10.1.4. Identity Awareness;
4.10.1.5. Application Control;
4.10.1.6. Content Awareness;
4.10.1.7. IPS;
4.10.1.8. URL Filtering;
4.10.1.9. Anti-Bot;
4.10.1.10. Anti-Virus;
4.10.1.11. Anti-Spam;
4.10.1.12. DNS Security;
4.10.1.13. SandBlast Threat Emulation;
4.10.1.14. SandBast Threat Extraction;
4.10.1.15. Zero-phishing;
4.10.1.16. SD-WAN;

4.11. ITENS 6 E 18 – SUBSCRIÇÃO FIREWALL TIPO III PARA 5 ANOS

4.11.1. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada:

4.11.1.1. Firewall;
4.11.1.2. VPN (IPsec);
4.11.1.3. Mobile Access;
4.11.1.4. Identity Awareness;
4.11.1.5. Application Control;
4.11.1.6. Content Awareness;
4.11.1.7. IPS;
4.11.1.8. URL Filtering;
4.11.1.9. Anti-Bot;
4.11.1.10. Anti-Virus;
4.11.1.11. Anti-Spam;
4.11.1.12. DNS Security;
4.11.1.13. SandBlast Threat Emulation;
4.11.1.14. SandBast Threat Extraction;
4.11.1.15. Zero-phishing;
4.11.1.16. SD-WAN;

4.12. ITENS 7 E 19 – SUBSCRIÇÃO FIREWALL TIPO IV

4.12.1. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada:

4.12.1.1. Firewall;
4.12.1.2. VPN (IPsec);
4.12.1.3. Mobile Access;
4.12.1.4. Identity Awareness;
4.12.1.5. Application Control;
4.12.1.6. Content Awareness;
4.12.1.7. IPS;
4.12.1.8. URL Filtering;
4.12.1.9. Anti-Bot;
4.12.1.10. Anti-Virus;
4.12.1.11. Anti-Spam;
4.12.1.12. DNS Security;
4.12.1.13. SandBlast Threat Emulation;
4.12.1.14. SandBast Threat Extraction;
4.12.1.15. Zero-phishing;
4.12.1.16. SD-WAN;

4.13. ITENS 8 E 20 – SUBSCRIÇÃO DE ENDPOINT

4.13.1. Deve possuir licenciamento por 60 (sessenta) meses, garantindo que a solução continue operacional, com todas as funcionalidades descritas nesse Termo de Referência habilitada;

4.13.2. Deverá ser entregue as licenças no quantitativo solicitado no Item 8 e Item 20 em portais separados para cada instituição:

4.13.2.1. Instituição Sesc Goiás;

4.13.2.1.1. Item 8 (1600 licenças);

4.13.2.2. Instituição Senac Goiás;

4.13.2.2.1. Item 20 (2000 licenças);

4.13.3. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

4.13.4. A solução de proteção avançada para notebooks, desktops e servidores consiste em um agente de segurança que será responsável pela análise de arquivos e comportamentos no sistema operacional do computador do usuário final ou servidor a fim de bloquear qualquer tipo de vulnerabilidade de dia-zero;

4.13.5. Deve escanear arquivos e identificar infecções baseado em características comportamentais dos vírus;

4.13.6. Deve escanear arquivos quando eles forem acessados, executados, permitindo detecção imediata e tratamento por qualquer ameaça;

4.13.7. Deve permitir executar uma análise detalhada de cada arquivo conforme selecionado pelo usuário;

4.13.8. Deve permitir especificar diretórios e extensões de arquivos para que sejam excluídos da análise de vírus;

4.13.9. Deve checar as áreas mais comuns do sistema de arquivos e a registry do sistema operacional em busca de ameaças avançadas;

4.13.10. Deve possuir as seguintes opções de remediação:

4.13.10.1. Reparar;

4.13.10.2. Quarentena;

4.13.10.3. Apagar;

4.13.11. Deve permitir ser gerenciado através de console unificada para gerenciamento centralizado de políticas e logs.

4.13.12. Deve identificar automaticamente o ponto de entrada do malware e o seu impacto para a organização;

4.13.13. A solução deve suportar os sistemas operacionais com versões mínimas de Windows 7 e Windows Server 2008 R2.

4.13.14. Deve gerar automaticamente relatório completo da execução do malware utilizando técnicas contidas no MITRE Framework;

4.13.15. Deve detectar ataques desconhecidos e de dia-zero. Arquivos copiados ou que tenha sido efetuado download devem ser enviados para emulação (sandboxing) em ambiente controlado a fim de detectar ataques de dia-zero;

4.13.16. Deve bloquear ataques independentemente se o vetor de distribuição é baseado na web, e-mail ou mídia removível;

4.13.17. Deve detectar e bloquear comunicações com servidores de comando e controle (C&C) para impedir vazamento de dados mesmo quando conectado/trabalhando remotamente. Deve permitir a quarentena de sistemas infectados para evitar que o malware se espalhe;

4.13.18. Deve possuir funcionalidade de análise forense de incidente, provendo uma visão completa do fluxo do ataque, causa raiz, impacto no negócio e o ponto de entrada do malware para agilizar as ações de remediação;

4.13.19. O Endpoint deve ser integrado ao Antivírus (agente único e gerenciamento), que fornece uma forte proteção de primeira linha estática e dinâmica usando assinaturas e análise comportamental;

4.13.20. Deve suportar emulação Threat sandbox, que inclui tecnologias de detecção para identificar malware desconhecido para o qual a assinaturas. Isso é realizado combinando recursos avançados de aprendizado de máquina, análise comportamental dinâmica de SO, identificando comportamentos suspeitos e mal-intencionados, táticas de hacking e técnicas de engenharia social, analisando as comunicações C&C durante a análise do sandbox e muito mais. O malware detectado é impedido de baixar (a sessão de download é interceptada pelo Endpoint). Se o malware já estiver na máquina, ele será colocado em quarentena;

4.13.21. A solução pode ser configurada para enviar arquivos para emulação no dispositivo de sandbox local e na nuvem;

4.13.22. Deve possuir prevenção contra malware de dia zero, realizando a extração de ameaças fornecendo arquivos higienizados para os usuários;

4.13.23. O produto deve suportar no mínimo dois modos básicos de higienização de arquivos:

4.13.23.1. Manter tipo de arquivo - entregar o arquivo em seu formato original, removendo qualquer conteúdo ativo, como macros;

4.13.23.2. Converter para PDF - os arquivos entregues aos usuários são convertidos para o formato PDF, uma transformação praticamente impossível para qualquer malware sobreviver. Dessa forma os usuários podem obter acesso auto-suficiente ao arquivo original, se tal acesso for necessário. O acesso é garantido apenas se o arquivo for limpo pelo mecanismo de detecção de emulação de ameaças;

4.13.24. O endpoint deve fornecer a capacidade de ativar / desativar granularmente cada funcionalidade, que serve como um meio para isolar qualquer interferência com outros aplicativos. Além das ferramentas de solução de problemas padrão, as informações de forense podem ajudar na identificação de tais interferências;

4.13.25. Deve ser capaz de efetuar roll-back de mudanças no registro do Windows e alterações no sistema de arquivos em caso de alteração a arquivos infectados;

4.13.26. Deve possuir extensão para navegador Internet, Google Chrome e Internet Explorer, para prevenir contra ameaças avançadas de dia-zero e extração de conteúdos maliciosos para os downloads efetuados via web pelos usuários;

4.13.27. Deve proteger os dados forenses armazenados na estação de trabalho (Endpoint) contra acessos não autorizados ou outro tipo de tentativa de manipulação através da estrutura segura de logs da solução;

4.13.28. Os clientes se comunicam apenas com servidores autorizados (ou seja, apenas IPs específicos fornecidos por um servidor autenticado) e realizam a validação do certificado do servidor (usando informações internas) para verificar se o servidor é confiável;

4.13.29. Deve possuir análise de campos de login e senha em caso de acesso a páginas de internet como e-mail e formulários na detecção e prevenção de sites de phishing;

4.13.30. Deve possuir mecanismo de proteção para evitar que o usuário use credenciais corporativas em sites não corporativos;

4.13.31. A solução deve ser capaz de fazer remediação de forma automatizada, sem a necessidade da intervenção do usuário;

4.13.32. A solução deverá detectar e bloquear tem tempo real qualquer ação maliciosa ao sistema operacional que venha através de download de arquivos na Web, cópia através de um drive externo, sites de phishing e até mesmo mecanismos de criptografia de arquivos como o Ransomware. Sendo que a solução deve possuir mecanismos de restauração dos arquivos no momento que é detectado e bloqueado o Ransomware, ou seja, não permitindo o sequestramento de informações;

4.13.33. A solução deverá detectar e bloquear ameaças em download ou através de movimento lateral (cópia de arquivos) em qualquer extensão Microsoft Office, sendo ela capaz de detectar qualquer tipo de executável que tente criptografar os arquivos do computador do usuário.

4.13.34. A solução deverá detectar e bloquear malwares dia zero no momento do download e cópia através de drive externo. Deve prevenir e remediar de forma automática ataques evasivos de Ransonware, baseado em análise comportamental;

4.13.35. Deve reverter as ações do Ransonware, restaurando os dados corporativos automaticamente, garantindo proteção contra criptografia dos dados;

4.13.36. Possuir tecnologia que não seja baseada em assinaturas, garantindo seu funcionamento tanto de forma online quanto offline;

4.13.37. Deve permitir que os agentes obtenham atualizações de assinaturas através de um ponto local, sem uma conexão com o serviço de gerenciamento;

4.13.38. Deve implementar, através de análise dinâmica e heurística, proteção em tempo real contra sites conhecidos e desconhecidos de phishing;

4.13.39. Deve detectar, através de análise estática e heurística, elementos suspeitos em sites que solicitem credenciais dos usuários;

4.13.40. Deve detectar e prevenir a reutilização de credenciais corporativas em sites externos;

4.13.41. Deve ser suportar o monitoramento do Log de Eventos do Windows para analisar eventos de malware de fornecedores de antivírus de terceiros;

4.13.42. Deve ser capaz de realizar ações com base no Log de Eventos do Windows, como:

4.13.42.1. analisar ataques;

4.13.42.2. encerrar processos;

4.13.42.3. excluir ou colocar arquivos em quarentena;

4.13.43. Deve possuir processo de análise forense automático de incidentes, disponibilizando as seguintes informações sobre o ataque:

4.13.43.1. Eventos Maliciosos;

4.13.43.2. Ponto de entrada do malware;

4.13.43.3. Escopo dos danos causados;

4.13.43.4. Máquinas infectadas;

4.13.44. Deverá ser capaz de realizar importação customizada de Indicadores de Comprometimentos (IOC) externos;

4.13.45. Gerenciamento Centralizado de políticas de Segurança, Logs e relatórios:

4.13.46. O Software de Gerência deve ser capaz de gerenciar todos os endpoint de Segurança de forma centralizada, possibilitando a concentração dos Logs e emissão de relatórios;

4.13.47. A gerência dos endpoints deve ser realizada através de console própria ou através de interface web (HTTPS);

4.13.48. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos;

4.13.49. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos;

4.13.50. Acesso avançado para monitorar e gerenciar as funções do sistema;

4.13.51. A solução deve ter integração com o Microsoft Active Directory para identificação de usuários;

4.13.52. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e análise dos eventos;

4.13.53. A solução de gerenciamento deverá ser entregue em nuvem do próprio fabricante, ou em appliance do próprio fabricante ou servidores de terceiros sendo eles listados em uma base de compatibilidade de hardware ou ambiente virtualizado;

4.13.54. A solução deve apresentar sumário apontando os agentes que estão instalados, em progresso ou que ainda estão pendentes;

4.13.55. A gerência deve apontar os agentes nos endpoints que foram violados com Segurança;

4.13.56. Todos os logs deverão ser referenciados com o nome do usuário devido a integração com o Active Directory;

4.13.57. A solução deve possuir outros módulos de Segurança onde podem ser incorporadas na mesma console de gerenciamento;

4.13.58. Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos;

4.13.59. Disponibilizar recursos interativos de navegação nos eventos informados;

4.13.60. A solução deve possuir relatórios customizáveis onde seja possível pegar diferentes informações para montagem do relatório;

4.13.61. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações: bloqueio da origem, envio de snmp e envio de e-mail;

4.13.62. A solução deve exportar relatórios via HTML e CSV;

4.13.63. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

4.13.64. A solução deve permitir o administrador ser capaz de atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes;

4.13.65. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:

4.13.65.1. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

4.13.65.2. Estatísticas com comparativo de período (hora, dia e mês);

4.13.66. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;

4.13.67. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e análise dos eventos;

4.13.68. Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por pais;

4.13.69. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.13.70. Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino;

4.13.71. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes;

4.13.72. Deve estar incluso no dashboard com horários predefinidos, diários, semanais e relatórios mensais. Incluindo:

4.13.72.1. Top eventos;

4.13.72.2. Top origem;

4.13.72.3. Top destinos;

4.13.72.4. Top Serviços;

4.13.72.5. Top origens e os seus principais eventos;

4.13.72.6. Top destinos e seus principais eventos;

4.13.73. Solução deve incluir relatórios de horários, diários, semanais e mensais pré-definidos. Incluindo pelo menos eventos Top origem, Top destino, Top evento, Top users, Top localidade de origem e os principais eventos relacionados em cada filtro;

4.13.74. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado;

4.13.75. A solução deve possuir pesquisa através de todos os endpoints instalados para buscar informações relacionadas a nome de processo, MD5 do arquivo, IP da rede origem, IP da rede de destino, URL, nome do arquivo, tipo do arquivo para identificação de possíveis atividades anômalas no ambiente corporativo;

4.13.76. A solução deve possuir pesquisa das principais atividades maliciosas, através de pesquisas baseadas em processos, palavras chaves ou usuário. Quando encontrado, deve ser possível incluir outras informações no campo de busca que podem ser combinadas no período determinado pelo administrador. Assim, terá ampla visibilidade da informação que foi colocado na busca em todos os endponits instalados no ambiente de produção;

4.13.77. A ferramenta deve apresentar linha do tempo com as principais atividades de rede e ameaças permitindo o administrador ter mais informações entre elas:

4.13.77.1. Detalhes da rede;

4.13.77.2. Detalhe do dispositivo identificando contendo informações do usuário, computador, OS Name, OS version, Domain Name e Host MACs;

4.13.77.3. Detalhes do processo que foi identificado através da busca realizada;

4.13.77.4. Horário da atividade que foi identificada;

4.13.78. Quando identifica qualquer atividade de rede ou ameaça através da ferramenta, a solução deve permitir o administrador a realizar ações como:

4.13.78.1. Terminar processo;

4.13.78.2. Quarentenar arquivo;

4.13.78.3. Ter acesso a análise forense;

4.13.79. Deverá permitir consultas predefinidas de vulnerabilidades reais, permitindo também uma visualização do painel MITTRE&ATTACK, ajudando na identificação das técnicas de evasão baseado neste framework;

4.13.80. Caso não seja o fabricante da solução, a licitante deverá apresentar declaração do fabricante da solução ofertada, dirigida a contratante, junto a proposta comercial, informando que é revenda autorizada no Brasil, estando apta a comercializar, prestar suporte e garantia dos produtos e serviços ofertados;

4.14. ITENS 9 E 21 – SERVIÇO GERÊNCIA E SUPORTE ESPECIALIZADO

4.14.1. Deverá ser fornecido serviço de suporte especializado durante o período de 12 meses, contados a partir da assinatura do contrato e/ou documento equivalente;

4.14.2. A CONTRATADA deverá monitorar, gerenciar e administrar remotamente todos os equipamentos de firewall adquiridos pelo CONTRATANTE através deste edital;

4.14.3. Será de dever da CONTRATADA realizar configurações preventiva e corretiva nos equipamentos adquiridos pelo CONTRATANTE através deste edital;

4.14.4. Ficará de responsabilidade da CONTRATADA realizar backup de todas as configurações realizadas nos equipamentos de firewall adquiridos pelo CONTRATANTE através deste edital;

4.14.5. A CONTRATADA deverá monitorar, gerenciar e administrar remotamente equipamentos e softwares componentes das soluções fornecidas e realizar a resposta a incidentes de segurança dos ativos fornecidos no serviço na rede do CONTRATANTE, 24 horas por dia, 7 dias da semana;

4.14.6. Esse serviço deverá ser realizado de forma local ou remota para assegurar que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos em regime 8x5 (8 horas por dia, 5 dias da semana), conforme a necessidade, exceto para o serviço de monitoramento de segurança que deverá operar em regime 24x7 (24 horas por dia, 7 dias da semana);

4.14.7. Implementar mecanismos para que ataques, invasões ou incidentes sofridos pelo CONTRATANTE em suas redes e/ou sistemas, sejam identificados, controlados, interrompidos ou cessados, em caráter provisório ou definitivo, mantendo o CONTRATANTE sempre a par de tais ocorrências;

4.14.8. Adotar, de imediato, as medidas de combate ao detectar tentativas de ataques. No caso dessas medidas implicarem em interrupções e/ou descaracterização dos serviços em uso, a empresa deverá entrar em contato com o CONTRATANTE para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las;

4.14.9. Monitorar o funcionamento de toda a solução deste Edital, 24 horas por dia, 7 dias da semana. Em caso de paralisação de equipamentos ou serviços monitorados, a equipe de especialistas da CONTRATADA deverá entrar em contato imediato com os responsáveis técnicos do CONTRATANTE informando o tipo de alerta e a solução do mesmo;

4.14.10. Caberá ao CONTRATANTE decidir pela implementação, ou não, de qualquer sugestão apresentada nos relatórios, assumindo a responsabilidade por problemas, que porventura vierem a ser causados nos equipamentos e serviços da rede, em função de ter optado por não acatar determinada recomendação;

4.14.11. Devem ser realizados testes de forma semestral e automatizados para avaliar o nível de segurança das camadas de segurança que protegem a rede DMZ e rede de usuários, podendo ser ferramentas de mercado ou de software livre;

4.14.12. Principais atividades a serem executadas de forma contínua pela CONTRATADA:

4.14.12.1. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

4.14.12.2. Monitorar permanente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;

4.14.12.3. Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;

4.14.12.4. Elaborar e propor plano de execução dos serviços;

4.14.12.5. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;
4.14.12.6. Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do Sesc e Senac Goiás, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
4.14.12.7. Receber as demandas dos serviços relativas à área de segurança da informação e providenciar a execução e alocação de recursos de trabalho;
4.14.12.8. Consolidar os relatórios de atividades mensais (mês calendário), referente aos Serviços Gerenciados de Segurança, provendo informações gerenciais ao CONTRATANTE;
4.14.12.9. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
4.14.12.10. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação e consolidá-las;
4.14.12.11. Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;
4.14.13. A contratada deverá criar rotina mensal de envio de relatórios para a CONTRATANTE contendo;
4.14.14. Histórico de navegação;
4.14.15. Top 10 endereços mais utilizados;
4.14.16. Sites bloqueados;

4.15. GARANTIA E SUPORTE

4.15.1. A CONTRATADA deverá prestar suporte técnico durante o período de 12 meses, contados a partir da assinatura do contrato e/ou documento equivalente;
4.15.2. O prazo de garantia será contado a partir do recebimento definitivo dos equipamentos ou solução;
4.15.3. Caso os equipamentos da CONTRATANTE sejam descontinuados na linha de fabricação do fabricante, durante a vigência do contrato e/ou documento equivalente de Suporte Técnico, a CONTRATADA deverá continuar a prestar o serviço de suporte técnico até o fim do contrato e/ou documento equivalente assinado junto a CONTRATANTE;
4.15.4. O Serviço de Suporte Técnico consiste essencialmente nos serviços de implantação de novos componentes da solução de Firewall Checkpoint, instalação, reinstalação, configuração, automatização de tarefas, aprimoramento de desempenho e resolução de incidentes e problemas (troubleshooting), procedimentos de melhorias, entre outros que sejam necessários ao perfeito funcionamento e gerenciamento da solução, atendendo às especificações técnicas do respectivo fabricante;
4.15.5. Os Serviços de Suporte Técnico deverão ser realizados por profissional da CONTRATADA, certificado na solução Checkpoint e suas blades, com qualificação e

treinamento adequados para o desenvolvimento das tarefas, com comprovação junto a proposta comercial de que possui em seu quadro profissional capacitado;

4.15.6. Os Serviços de Suporte Preventivo, deverão ser prestados durante a vigência do contrato e/ou documento equivalente, em regime 8x5, ou seja, de segunda a sexta-feira das 08:15 às 12:30 horas e das 14:00 às 18 horas, excluídos os feriados e fins de semana, em datas e horários acordados previamente com o CONTRATANTE e disponibilizados na forma de uma Agenda de Inspeções Técnicas;

4.15.7. Os Serviços de Suporte Corretivo deverão ser prestados sempre que solicitados pela CONTRATANTE, em regime 24x7, por meio da abertura de chamado técnico via Central de Atendimento;

4.15.8. Os Serviços de Suporte Programado deverão ser prestados sempre que solicitados pela CONTRATANTE, em regime 24x7, por meio da abertura de chamado técnico via Central de Atendimento;

4.15.9. Para os serviços descritos neste Termo de Referência, a CONTRATANTE garantirá o acesso físico dos técnicos especializados habilitados e identificados da CONTRATADA às instalações para execução dos serviços, caso sejam realizados de forma presencial. Esses técnicos ficarão sujeitos a todas as normas internas de segurança da CONTRATANTE, inclusive aqueles referentes à identificação, aos trajes, ao trânsito e à permanência em suas dependências;

4.15.10. Os Serviços de Suporte Técnico (Preventivo, Corretivo, Programado) poderão ser prestados de forma remota, excetuando-se os casos em que seja necessária a intervenção física do profissional nos equipamentos para a execução completa das tarefas de suporte ou, não seja possível acessar a rede de dados da CONTRATANTE;

4.15.11. Caso a CONTRATADA preste os serviços de forma remota, ela deverá prestá-los por meio do uso de ferramenta específica para este fim (acesso remoto) que garanta a confidencialidade, autenticidade e integridade no acesso, devendo ser por ela mesmo disponibilizada sem que sejam necessárias grandes alterações em políticas de segurança de rede de dados da CONTRATANTE;

4.15.12. A CONTRATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento de Chamados em língua portuguesa (telefone, sistema WEB ou e-mail), constituída de estrutura de pronto atendimento em regime 24x7, inclusive sábados, domingos e feriados, para abertura de chamados e consultas com técnico especializado na solução de Firewall Checkpoint e suas blades, em uso pela CONTRATADA, com conhecimento para solucionar problemas e esclarecer dúvidas, de forma rápida e eficiente;

4.15.13. Um chamado somente poderá ser fechado após confirmação do Gestor do contrato e/ou documento equivalente e apresentação do Relatório de Suporte elaborado pelo Responsável Técnico, sendo que o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de operação e de uso;

4.15.14. A classificação de uma solicitação de suporte técnico a um incidente deverá estar de acordo com o estabelecido na tabela abaixo:

4.15.15. Quando solicitada a CONTRATADA deverá elaborar um relatório com uma medição dos serviços realizados, que tomará como referência as Solicitações de Atendimento, os Relatórios de Suporte (intervenção corretiva e de intervenção programada) e o resultado apurado da efetiva prestação do serviço a ser registrado em Relatório de Atividades circunstanciado;

4.15.16. O Relatório deverá ser emitido pelo Preposto da Contratada, contendo no mínimo:

NÍVEL	CLASSIFICAÇÃO	DIAGNÓSTICO E SLA
1	CRÍTICO	A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 02 (duas) horas, contadas a partir da abertura do chamado de suporte corretivo pela CONTRATANTE. No prazo máximo de 8 (oito) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional, estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante.
2	URGENTE	A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 4 (quatro) horas, contadas a partir da abertura do chamado de suporte corretivo pela CONTRATENTE. No prazo máximo de 10 (dez) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional e sem nenhuma degradação, estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante.
3	ROTINA	A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 8 (oito) horas contadas a partir da abertura do chamado de suporte corretivo pela CONTRATANTE. No prazo máximo de 10 (dez) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional e sem nenhuma degradação, estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante.
4	PROGRAMADA	A CONTRATADA deverá iniciar o atendimento do chamado no prazo máximo de 48 (quarenta e oito) horas contadas a partir da abertura do chamado de suporte programado pela CONTRATENTE. No prazo máximo de 96 (noventa e seis) horas subsequentes ao início do atendimento do chamado, a CONTRATADA

		deverá entregar o cronograma com a descrição dos procedimentos a serem adotados para a solução completa do chamado de suporte programado.

4.15.17. Identificação do Relatório de Atividades;
4.15.18. Data de Emissão;
4.15.19. Número do Contrato e/ou documento equivalente;
4.15.20. Período de Referência;
4.15.21. Número e descrição dos chamados em aberto;
4.15.22. Suportes corretivos abertos no período de referência, com suas respectivas datas e horários de abertura e de início e término do atendimento, severidade e a descrição resumida dos problemas encontrados;
4.15.23. Suportes programados abertos no período de referência, com suas respectivas datas e horários de abertura do chamado e de entrega dos cronogramas e a descrição resumida das solicitações;

5. CRITÉRIO DE JULGAMENTO

5.1. Observadas às demais condições deste Termo de Referência, o julgamento deste certame será feito pelo critério **menor preço por LOTE (ÚNICO)**.

6. CONDIÇÕES PARA EXECUÇÃO DO OBJETO

6.1. Execução dos Serviços e Prazo de Entrega
6.1.1. Após a assinatura do contrato e/ou documento equivalente, a Contratada terá como prazo de entrega dos itens conforme listado abaixo:
6.1.1.1. Para os itens 1, 2, 3, 4, 10, 11, 12, 13 e 14 a Contratada possui um prazo de até 90 (noventa) dias úteis para entrega contados a partir da assinatura do contrato e/ou documento equivalente;
6.1.1.2. Para os itens 5, 6, 7, 8, 9, 15, 16, 17, 18, 19, 20 e 21 a Contratada possui um prazo de até 120 (cento e vinte) dias úteis para entrega contados a partir da assinatura do contrato e/ou documento equivalente;
6.1.2. Os pagamentos para os itens 01, 02, 03, 04, 05, 06, 07, 08, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 e 20 serão realizados em até 15 (quinze) dias subsequentes a entrega da nota fiscal e termo de aceite que comprovam o recebimento dos equipamentos e/ou execução dos serviços contratados pelo Sesc e Senac GO;
6.1.3. Os pagamentos para os itens 09 e 21 serão realizados mensalmente em até 15 (quinze) dias subsequentes a entrega da nota fiscal e termo de aceite que comprovam o recebimento dos equipamentos e/ou execução dos serviços contratados pelo Sesc e Senac GO;
6.1.4. Todas as despesas e custos diretos e indiretos necessários à prestação dos serviços do objeto ora licitados correrão inteira e exclusivamente por conta da Contratada;

6.1.5. O prazo de vigência do contrato e/ou documento equivalente a ser celebrado é de 12 (doze) meses, contados a partir da assinatura do contrato e/ou documento equivalente, podendo ser prorrogado igual período até o limite de 120 (centro e vinte) meses, em atendimento às necessidades e conveniência das partes envolvidas, observadas as justificativas técnicas invocadas e resguardadas as demais condições contratuais originais, desde que a prorrogação seja assegurada pelos instrumentos jurídicos, com suas alterações e eventuais aditamentos, que fundamentam essa contratação;

6.1.6. Cabe à Contratada o cumprimento dos prazos de entrega do objeto nas condições e locais definidos e nas quantidades contratadas, a contar da data da assinatura do contrato e/ou documento equivalente;

6.1.7. A Contratada cumprirá fielmente com as obrigações assumidas podendo sofrer penalidades previstas em caso de não cumprimento do estabelecido;

7. LOCAIS DE ENTREGA, EXECUÇÃO DO SERVIÇO E FATURAMENTO

7.1. Local de Entrega e Execução do Serviço - Itens 01 a 09.
SERVIÇO SOCIAL DO COMÉRCIO - SESC
Endereço: Rua 31-A, número 43, Setor Aeroporto, Goiânia – GO.
CEP: 74.075-470

7.2. Local de Entrega e Execução do Serviço - Itens 10 a 21.
SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC
Endereço: Rua 31-A, nº 43. Setor Aeroporto, Goiânia/GO.
CEP: 74075-470

7.3. Local de Faturamento - Itens 01 a 09.
Razão Social: Serviço Social do Comércio - Sesc
CNPJ: 03.671.444/0001-47
Inscrição Estadual: Imune
Endereço: Avenida 136, nº 1.084, Qd, F47, Lt. 3-5-7, Setor Marista, Goiânia – GO.
CEP: 74.180-040

7.4. Local de Faturamento - Itens 10 a 21.
Razão Social: Serviço Nacional de Aprendizagem Comercial - Senac
CNPJ: 03.608.475/0001-53
Inscrição Estadual: Imune
Endereço: Rua 31-A, número 43, Setor Aeroporto, Goiânia – GO,
CEP: 74.075-470.

8. EXIGÊNCIA DE HABILITAÇÃO

8.1. Documentos relativos à Habilitação Jurídica:

a) Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e no caso de sociedades por ações, acompanhado dos documentos de eleição dos seus administradores e respectivas alterações, se houver, podendo ser substituídos por certidão simplificada expedida pela Junta Comercial da sede da licitante; ou

b) Comprovante de inscrição do Ato Constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício. Este documento poderá ser substituído por certidão, em breve relatório, expedida pelo Registro Civil das Pessoas Jurídicas.

c) Documento comprobatório do representante legal da licitante:

1) Cópia da cédula de identidade do representante legal.

2) Procuração, caso a licitante se faça representar por procurador.

8.2. Documentos relativos à Regularidade Fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda - CNPJ.

b) Prova de inscrição no Cadastro de contribuintes Estadual e Municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

c) Certidão Conjunta Negativa ou Positiva com Efeitos de Negativa, de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, que abrange inclusive as contribuições sociais;

d) Certidão negativa ou positiva com efeito de negativa, de débitos junto à fazenda estadual;

e) Certidão negativa ou positiva com efeito de negativa, de débitos junto à fazenda municipal;

f) Certidão de Regularidade Fiscal (CRF) junto ao Fundo de Garantia por Tempo de Serviço (FGTS), no cumprimento dos encargos instituídos por lei; (exceto para Microempreendedor Individual-MEI).

8.3. Documentos relativos à Qualificação Econômico-Financeira:

a) Certidão negativa de falência ou concordata, expedida pelo órgão competente ou cartório distribuidor da sede do licitante, emitida a menos de 90 (noventa) dias da data de abertura do certame.

8.4. Documentos relativos à Regularidade Trabalhista:

a) Certidão Negativa de Débitos Trabalhistas – CNDT, expedida pelo Tribunal Superior do Trabalho.

8.5. Documentos relativos à Habilitação Técnica:

a) Comprovação da capacitação técnico-operacional, mediante apresentação de um ou mais atestados de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, comprovando que a Licitante forneceu objeto de natureza

semelhante ao da licitação, sem qualquer restrição na qualidade dos materiais e serviços, bem como nas condições comerciais, devendo conter:

1) o nome, o endereço e o telefone de contato do atestante, ou qualquer outra forma de que a Contratante possa valer-se para manter contato com a empresa declarante, comprovando obrigatoriamente em cada um dos atestados;

2) O atestado deverá referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente da licitante;

3) Prestação de serviços de suporte técnico à solução de FIREWALL CHECK POINT, em ambiente corporativo, na modalidade 24 x 7 (vinte e quatro horas, sete dias por semana) na língua portuguesa (brasil);

b) Entende-se por atividade pertinente e compatível com o objeto da licitação, o fornecimento de pelo menos 50% do total exigido neste Termo de Referência;

c) Deverá apresentar carta do fabricante dirigida ao Sesc Goiás e Senac Goiás, citando o número do processo licitatório junto a proposta comercial, confirmando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, suporte e garantia;

d) A Comissão de Licitação se reserva o direito de promover diligências através de contatos com o cliente, para certificar-se da exatidão das informações constantes dos atestados e/ou certificados apresentados pelas licitantes;

e) Qualquer informação inexata ou inverídica apurada pela Comissão de Licitação, constante dos documentos de capacitação técnica, implicará na inabilitação da respectiva LICITANTE;

f) No caso de atestados emitidos por empresa de iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa licitante;

g) Serão consideradas como pertencentes ao mesmo grupo empresarial, empresas controladas ou controladoras da empresa licitante, ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa licitante.

h) Qualquer informação inexata ou inverídica apurada pela comissão, constante dos documentos de capacitação técnica, implicará na inabilitação da respectiva LICITANTE.

9. GARANTIA DA EXECUÇÃO CONTRATUAL

9.1. No momento da assinatura do contrato e/ou documento equivalente para fiel cumprimento das obrigações assumidas, a Contratada prestará garantia correspondente a 5% (cinco por cento) do valor do contrato e/ou documento equivalente, nos termos do Art. 27 da Resolução Sesc nº 1.252/2012 e Resolução Senac nº 958/2012, em uma das seguintes modalidades:

a) Caução em dinheiro;

b) Seguro garantia; ou

c) Fiança bancária.

9.2. A garantia será realizada para assegurar o pagamento de:
a) Prejuízos advindos do não cumprimento do contrato e/ou documento equivalente;
b) Multas punitivas aplicadas à licitante Contratada;
c) Prejuízos diretos causados aos Contratante decorrentes de culpa ou dolo durante a execução do contrato e/ou documento equivalente.
9.2.1. A garantia prestada pela Contratada será liberada ou devolvida após requerida sua devolução no prazo máximo de 90 (noventa) dias e desde que o contrato e/ou documento equivalente esteja encerrado e todas as obrigações dele decorrentes tenham sido cumpridas.

10. OBRIGAÇÕES ENTRE AS PARTES

10.1. OBRIGAÇÕES DA CONTRATADA

10.1.1. Cabe a Contratada o cumprimento dos prazos de entrega, nas datas, condições e local definido, nas quantidades contratadas.
10.1.2. A Contratada cumprirá fielmente com as obrigações assumidas por meio deste Termo de Referência, podendo a contratante aplicar as penalidades cabíveis previstas.
10.1.3. Em nenhuma hipótese a Contratada poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe especificado neste Termo de Referência.
10.1.4. Correrá por conta da Contratada qualquer prejuízo causado ao material em decorrência de transporte.
10.1.5. Cabe a Contratada responsabilizar-se por despesas, tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal e quaisquer outras que incidam ou venham a incidir na execução da Ata de Registro de Preço.
10.1.6. Atender prontamente a quaisquer exigências do Sesc e Senac Goiás, inerentes ao objeto do presente Termo de Referência.

10.2. OBRIGAÇÕES DA CONTRATANTE

10.2.1. Os pagamentos para os itens 01, 02, 03, 04, 05, 06, 07, 08, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 e 20 serão realizados em até 15 (quinze) dias subsequentes a entrega da nota fiscal e termo de aceite que comprovam o recebimento dos equipamentos e/ou execução dos serviços contratados pelo Sesc e Senac GO.
10.2.2. Os pagamentos para os itens 09 e 21 serão realizados mensalmente em até 15 (quinze) dias subsequentes a entrega da nota fiscal e termo de aceite que comprovam o recebimento dos equipamentos e/ou execução dos serviços contratados pelo Sesc e Senac GO.
10.2.3. Prestar aos empregados da Contratada informações e esclarecimentos que eventualmente venham ser solicitados, e que digam respeito a natureza do fornecimento.

10.2.4. Caberá ao Sesc e Senac Goiás notificar a Contratada, por escrito, quaisquer falhas, erros, imperfeições ou irregularidades que encontrar no serviço/ objeto fornecidos, bem como, exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com este termo de referência e demais normas da Entidade.

10.2.5. Permitir aos funcionários da Contratada, o aceso as instalações relativas ao objeto do presente Termo de Referência, para efeito de execução do fornecimento, durante o expediente norma de funcionamento dos serviços.

10.2.6. Acompanhar e fiscalizar o exato cumprimento das condições estabelecidas neste Termo de Referência.

10.2.7. A Fiscalização e o acompanhamento da execução do contrato e/ou documento equivalente por parte do Contratante não excluem nem reduz a responsabilidade da Contratada em relação ao mesmo

10.2.8. O Sesc e o Senac Goiás reservam o direito de não receber e/ou atestar a prestação de serviço em desacordo com as especificações e condições constantes neste Termo, podendo aplicar as penalidades cabíveis.

10.2.9. Será designado representante para acompanhar e fiscalizar a realização do serviço e/ou entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário a regularização de falhas ou defeitos observados.

11. DA SUBCONTRATAÇÃO

11.1. Será admitida a subcontratação dos serviços, restrita, contudo, ao percentual máximo de 30% (trinta porcento) do orçamento, devendo o contratado apresentar a documentação que comprove a qualificação técnica necessária da empresa a ser subcontratada;

11.2. A subcontratação depende de autorização prévia do Sesc e Senac Goiás, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do objeto;

11.3. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

12. DA ADESÃO AO REGISTRO DE PREÇO

12.1. A Ata de Registro de Preços poderá ser objeto de adesão pelo Departamento Nacional do Sesc e Senac (DN), Departamento Regional do Sesc e Senac (DR) com jurisdição em qualquer das bases territoriais correspondentes, bem como, por todo serviço social autônomo, desde que nas mesmas condições firmadas com o Sesc Goiás, nos termos da Resolução 1.252/2012 (Regulamento de Licitações e Contratos

do Sesc); e do Senac Goiás, nos termos Resolução 958/2012 (Regulamento de Licitações e Contratos do Senac);

12.2. O Aderente informará ao Gerenciador o seu interesse em aderir a Ata de Registro de Preço;

12.3. O Gerenciador indicará ao Aderente os quantitativos de bens/serviços previstos no instrumento convocatório, o fornecedor, as condições em que tiver sido registrado o preço e o prazo de vigência do registro;

12.4. As aquisições por Aderente não poderão ultrapassar 100% dos quantitativos previstos no instrumento convocatório;

12.5. As razões da conveniência de aderir ao registro de preço cabem ao Aderente;

12.6. O pedido de adesão ao Gerenciador e a contratação da aquisição de bens ou serviços pelo Aderente com o fornecedor deverão ser realizadas durante a vigência do registro de preço;

12.7. O fornecimento ao Aderente deverá observar as condições estabelecidas no registro de preço e não poderá prejudicar as obrigações assumidas com o Gerenciador e com os Aderentes anteriores;

12.8. O fornecedor poderá optar por não contratar com o Aderente.

13. DA PROPOSTA

13.1. A proposta deverá ser elaborada em papel timbrado, datada, obedecendo ao Termo de Referência e seus anexos;

13.2. Deverá Conter preço unitário por item e valores totais, indicados em moeda corrente nacional (com apenas duas casas decimais após a vírgula), sendo preços fixos e irreajustáveis, incluindo todos e quaisquer impostos incidentes, descontos, frete, mão de obra, emolumentos, contribuições previdenciárias, fiscais, sociais e parafiscais, que sejam devidos em decorrência, direta ou indireta, da entrega do objeto da presente licitação;

13.3. Razão Social completa da licitante e CNPJ, os quais deverão ser os mesmos constantes da documentação;

13.4. Valor total que será expresso em real e por extenso.

13.5. O prazo de validade da proposta, não poderá ser inferior a 90 (noventa) dias;

13.6. A omissão de qualquer uma das exigências desta solicitação, será considerado o aceite a todas as condições estabelecidas neste Termo de Referência, não podendo ser alegado desconhecimento do mesmo;

13.7. A proposta deverá conter a descrição detalhada com marca/modelo, códigos do fabricante de todos os módulos, fontes e acessórios fornecidos, apresentada com uma planilha ponto a ponto, junto a proposta comercial, que comprove o atendimento dos requisitos, indicando a página da documentação técnica onde consta o requisito

14. DAS PENALIDADES

14.1. Em caso de inadimplemento total, parcial, sem motivo de força maior, a licitante estará sujeita, no que couber, e garantida a prévia defesa, às penalidades previstas na legislação aplicável, para as seguintes hipóteses:

14.1.1. Por atraso injustificado ou por inexecução parcial:

a) Advertência;

b) Multa de 0,3% (zero vírgula três por cento) ao dia incidente sobre o valor correspondente ao material ou serviço objeto desta licitação;

c) Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc e/ou Senac, por um prazo de até 2 (dois) anos.

14.1.2. Por inexecução total do objeto desta licitação:

a) Advertência;

b) Multa de 10% (dez por cento) sobre o valor total do contrato e/ou documento equivalente; e

c) Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc e/ou Senac/GO, por um prazo de até 2 (dois) anos;

14.2. As multas estabelecidas neste item são independentes e terão aplicação cumulativa e consecutivamente, de acordo com as normas que regeram a licitação, mas somente serão definitivas depois de exaurida a fase de defesa prévia da empresa adjudicada.

14.3. Quando não pagos em dinheiro pela empresa adjudicada, os valores das multas eventualmente aplicadas serão deduzidos pelo Sesc e/ou Senac, dos pagamentos devidos e, quando for o caso, cobrado judicialmente.

14.4. Quando se tratar de inexecução parcial, o valor da multa será proporcional ao serviço que deixou de ser executado.

14.5. Caso haja a recusa injustificada em assinar o contrato e/ou documento equivalente no prazo de 03 (três) dias úteis, a contar da data da convocação, a empresa estará sujeita a penalidade prevista no 14.1.2, alínea "c" e dará ao Sesc e/ou Senac GO o direito de homologar e adjudicar esta licitação aos licitantes remanescentes, na ordem de classificação.

14.6. O prazo de convocação para assinatura do contrato e/ou documento equivalente poderá ser prorrogado uma vez, por igual período, quando solicitado pela empresa, durante o seu transcurso, desde que ocorra motivo justificado e aceito pelo Sesc e/ou Senac/GO.

14.7. Em caso de reincidência por atraso injustificado será a empresa penalizada nos termos do art. 32, da Resolução Sesc/GO nº. 1252/2012 e Senac/GO nº 958/2012.

15. FISCALIZAÇÃO

a) Fiscal

Lucas Reges Barros
Matrícula: 5548
Cargo: Analista de Redes
CPF: xxx.xxx.xxx-75

b) Suplente
Jean Franklin Silva Pereira
Matrícula: 11116
Cargo: Analista de Redes
CPF: xxx.xxx.xxx-68

16. RESPONSÁVEL TÉCNICO

Saúle Tassara Bortolani
Matrícula: 5502
Cargo: Líder Seção Infraestrutura e Suporte TI
CPF: xxx.xxx.xxx-91

17. RESPONSÁVEIS PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

Lucas Reges Barros
Analista de Redes

Jean Franklin Silva Pereira
Analista de Redes

Karlla Cristhina Rodarte
Líder Seção Infraestrutura e Suporte TI – e.e.

Saúle Tassara Bortolani
Diretor de Transformação Digital e Inovação – e.e.

Goiânia, 21 de novembro de 2023.