TERMO DE REFERÊNCIA

1. INFORMAÇÕES PRIMÁRIAS:

Órgão Requerente: *- Secretaria Municipal de Administração.*	Descrição de categoria de investimento: **( ) Aquisição** **(x) Contratação de Serviços**

2. MODALIDADE E O TIPO DE LICITAÇÃO:

Modalidade de Licitação:	**Tipo de Licitação:**
(X) PREGÃO ELETRÔNICO amparo legal Lei Federal 14.133/2021; ( ) CONCORRÊNCIA amparo legal Lei Federal 14.133/2021; ( ) CONCURSO amparo legal Lei Federal 14.133/2021; ( ) LEILÃO amparo legal Lei Federal 14.133/2021; ( ) DIÁLOGO COMPETITIVO amparo legal Lei Federal 14.133/2021; PROCEDIMENTO DE CONTRATAÇÃO DIRETA ( ) DISPENSA amparo legal Lei nº 14.133/2021 artigo 75 ( ) INEXIGIBILIDADE amparo legal Lei Federal 14.133/2021 Artigo 74.	Lei Federal 14.133/2021: **(X) Menor Preço Lote;** ( ) Maior Desconto Global por Item; ( ) Melhor Técnica; ( ) Técnica e Preço; ( ) Maior lance; ( ) Maior Retorno ( ) Outros

3. DA LEGISLAÇÃO APLICÁVEL:

(X) Lei Federal n° 14.133/2021 e suas alterações (Institui normas para Licitações e Contratos da Administração);
(X) Decreto Municipal nº 903/2023 que regulamenta a Lei Federal 14.133/2021 no Município de Sorriso – MT;
( ) Lei Complementar n°123/2006 (Institui o Estatuto Nacional da Microempresa e Empresa de Pequeno Porte) e alterações posteriores;
(X) E demais disposições a serem estabelecidas no Edital de Licitação e em seus Anexos..

4. DO OBJETO:

O presente Termo de Referência tem por finalidade definir o conjunto de elementos que nortearão o procedimento para o "**CONTRATAÇÃO DE EMPRESA PARA LOCAÇÃO EQUIPAMENTO DE SEGURANÇA DO TIPO FIREWALL PARA SEGURANÇA DA INFORMAÇÃO COMPOSTA DE APPLIANCE FÍSICA E SOFTWARE COM LICENCIAMENTO DE USO POR 36 MESES INCLUINDO INSTALAÇÃO, ATUALIZAÇÃO E CONFIGURAÇÃO DA FERRAMENTA COM REPASSE DE CONHECIMENTO PARA COLABORADORES E SUPORTE TÉCNICO SOB DEMANDA COM DURAÇÃO DE 36 MESES",** conforme condições, quantidades necessárias.

5. DA JUSTIFICATIVA:

- FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Tecnologia da Informação é um dos principais agentes de mudanças organizacionais. Sua utilização deve atentar-se para as questões estratégicas de apoio a integração operacional, organizacional e funcional. A correta utilização dos recursos da tecnologia contribui para um ambiente institucional moderno integrando as ações de todos os setores, fazendo da informatização um fator crítico de sucesso institucional.

Nos últimos anos nossa preocupação em relação ao controle e gerenciamento de dados em nossa instituição aumentou. Os pilares de segurança da informação sofreram alterações na era da informação, sendo eles caracterizados pelos seguintes atributos: disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio. Segurança é um processo contínuo que não se conclui. Novos tipos de ataques cibernéticos são descobertos quase que diariamente. Vulnerabilidades de softwares são divulgadas todos os dias. Os processos referentes à segurança precisam ser revistos diariamente através de relatórios e acompanhamentos, e obviamente, os softwares envolvidos com a segurança da rede de dados precisam ser atualizados na mesma velocidade.

Firewall é um dispositivo composto de software e/ou hardware, que limita o acesso à rede, dando credenciais de acesso apenas a aqueles que realmente devem fazer o acesso à informação. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados na rede. O firewall pode ser usado para ajudar a impedir que a rede ou um computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers. O firewall é um grande aliado no que se refere à segurança da informação, uma vez que é capaz de bloquear vulnerabilidades que, eventualmente, sejam usadas para a entrada de "pragas digitais", é possível realizar o controle a nível de aplicação através de bloqueio ao acesso de programas não autorizados.

A compra mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede mundial de computadores (internet). Atualmente, são diversos os tipos de ataques que são conhecidos na internet e ainda, assim, hackers conseguem obter sucesso pela não prevenção e a presença de equipamentos modernos e ativos que minimizam estes riscos, sendo assim, a Prefeitura de Sorriso, no intuito de aprimorar seus fundamentos de segurança da informação, tem como objetivo contratar não somente os ativos de rede (firewalls), mas, também, o suporte e garantia da solução, mantendo a base de ameaças atualizada, garantindo assim a proteção de seu bem mais precioso que são as informações armazenadas.

Contratação de empresa mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede mundial de computadores (internet), no fornecimento de solução de segurança da informação (Firewall fornecimento de solução de segurança da informação (Firewall) para proteção de acessos à rede intranet (interna) e WAN (externa), no intuito de garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Prefeitura Municipal de Sorriso, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação dessa instituição. Atualmente, a Prefeitura utiliza a solução de Firewall FortGate 80F, o que está no limite de sua totalidade de gerenciamento devido ao aumento significativo de usuários e equipamentos na intranet, diante da dimensão e fluxo de tráfegos na rede da Prefeitura Municipal de Sorriso.

A atual ferramenta de segurança da informação não permite obter uma visão mais detalhada do tráfego a nível das aplicações que estão trafegando dados, qual o nível de risco do tráfego e se ele pode trazer ameaças para a rede. Esse tipo de informação é muito importante para prover uma rápida análise caso ocorra algum incidente e para a geração de relatórios sobre uso da banda, o que auxilia a diagnosticar de forma rápida e eficiente as causas de possíveis ataques cibernéticos ou lentidão na rede. Além disso, com base na maior utilização de dispositivos e sistemas computacionais, é importante observar o aumento da demanda de uso da banda de Internet existente na Prefeitura Municipal de Sorriso. Isso se deve ao fato de que, com o passar dos anos, a infraestrutura de Tecnologia da Informação e Comunicação desta Instituição cresceu muito com a ampliação de equipamentos e usuários, bem como permitindo a proliferação dos dispositivos pessoais dentro desta Infraestrutura através de rede wi-fi corporativa gerenciada, e considerando a evolução das aplicações e métodos de criptografia SSL utilizados na maioria das conexões existentes acarretou em extrema complexidade para a gestão da segurança da Informação. Em virtude desse maior consumo da banda, a solução de firewall atual sofre

problemas de performance, apresentando gargalos de processamento e gerenciamentos de pacotes.

A solução de firewall atual não será mais compatível para um aumento de equipamentos e usuários, pois, atualmente a solução em questão já trabalha com o máximo da sua capacidade. Nesse caso, isso ocasionaria frequentes perdas e necessidade de retransmissão de pacotes, o que reflete em atrasos no tráfego de dados, ou seja, uma lentidão na rede, a qual pode ser percebida pelos usuários em momentos de maior utilização.

Equipamentos de segurança do tipo firewall NGFW para segurança da informação composta por uma appliance física e software com licenciamento de uso para de 36 meses, distribuídos no processo em lote único com três itens distintos, (conforme detalhado neste documento), incluindo o suporte preventivo e corretivo 24x7, monitoramento com alertas via e-mail e/ou sms, Operação e Backup online das configurações do equipamento.

Deste modo, após análise e avaliação crítica da cesta de preços que será realizada, o critério utilizado para a definição do preço de referência será a média de todos os valores obtidos.

- OBJETIVOS A SEREM ALCANÇADOS

Na estruturação da rede de informática da prefeitura, considerando o avanço da legislação no que se refere às políticas de segurança da informação, é necessário ampliar a estrutura de tecnologia, já que desde 2017 até o momento diversos setores e departamentos surgiram, aumentando o número de usuários e consequentemente a informação que precisa ser tratada.

Dentro desta lógica de avanço tecnológico e obtenção de novas ferramentas que visam tanto a melhoria interna (qualidade e segurança) e externa (melhor atendimento ao contribuinte), o presente processo trata de aquisição de solução completa de FIREWALL NGFW, necessário para atender as necessidades da prefeitura. Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração possibilita a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso seria possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Assim, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes. Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões. Essas informações são extremamente importantes, seja para realizar a adequação ao Marco Civil da Internet ou para realizar o tratamento de incidentes de segurança. No cenário atual, essas informações muitas vezes são ineficientes, visto que a arquitetura implementada não está possibilitando armazenar esses dados. Um firewall de próxima geração oferece isso de forma interessante, sendo possível gerar relatórios de forma rápida e detalhada sobre tudo o que acontece na rede. Dessa forma, o firewall possibilitará manter e ampliar aos seguintes resultados:

- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de
- Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
- Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
- Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
- Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários etc.
- Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
- Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
- Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.
- Utilização do firewall atenda as demandas da Prefeitura Municipal de Sorriso, diminuindo riscos de indisponibilidades, imprevistos e ataques.

- Cumprir o princípio da economicidade com os recursos financeiros desta Prefeitura, buscando no mercado atual um preço justo e competitivo.
- A utilização de sistemas por partes dos munícipes com alta segurança na transação de informações via internet.
- Possibilidade de visão de tráfego a nível das aplicações que estão trafegando os dados.

6. DA ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS:

6.1. Equipamentos de segurança do tipo firewall NGFW para segurança da informação composta de appliance físico, o software com licenciamento de uso para no mínimo 36 meses, salvamento de logs e atualizações, incluindo instalação/configuração da ferramenta e repasse de conhecimento para o Departamento de TI e suporte técnico sob demanda, **CONFORME AS ESPECIFICAÇÕES DO ANEXO I**:

7. VALOR ESTIMADO DA CONTRATAÇÃO:

7.1. Secretaria Municipal de Administração: R$ 1.216.492,13 (Um milhão duzentos e dezesseis mil quatrocentos e noventa e dois reais e treze centavos).

7.2. Cesta de preços obtida através de cotações em empresas especializadas, sistema Radar TCE-MT, Painel de preços e sistema Banco de Preços, sendo:

- AIM7 COMÉRCIO E SERVIÇOS DE INFORMÁTICA - CNPJ: 07.590.774/0001-69;
- JRV SERVIÇOS LTDA - CNPJ: 08.208.805/0001-37;
- RELIEVE SOLUÇÕES EM TECNOLOGIA LTDA - CNPJ: 44.687.774/0001-08;
- CONTROLADORIA GERAL DA UNIÃO - CGU – Pregão Eletrônico N° 90001/2024;
- INSTITUTO FEDERAL DE RORAIMA - CAMPO ZONA OESTE Pregão Eletrônico N° 11/2023;
- UNIVERSIDADE FEDERAL DE MINAS GERAIS - Pregão Eletrônico N° 05/2023;
- PREFEITURA MUNICIPAL DE PRIMAVERA DO LESTE - Pregão Eletrônico N° 79/2023;
- CONSELHO REGIONAL DE EDUCAÇÃO FISICA DA PRIMEIRA REGIÃO - Pregão Eletrônico N° 07/2023.

7.3. Após análise e avaliação crítica da cesta de preços realizada, o critério utilizado para a definição do preço de referência foi a média entre os valores, devido a especificidade do objeto, visto que, o sistema Radar TCE-MT, Painel de preços e sistema Banco de Preços, não encontramos critérios específicos do item, sendo necessário o orçamento por empresa especializadas.

8. DOTAÇÃO ORÇAMENTÁRIA:

8.1. Conforme anexo II.

9. PRAZOS E FORMA DE EXECUÇÃO:

9.1. EXECUÇÃO

- Realização da Reunião Inicial
  - Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou de forma remota. Na reunião inicial:
    - O representante legal da contratada deverá entregar o Termo de Compromisso e o Termo de Ciência, contendo declaração de

manutenção de sigilo e respeito às normas de segurança vigentes na entidade;
- O representante legal da contratada deverá apresentar o cronograma de execução do projeto;
- Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

- Prazos, horários de fornecimento de bens ou prestação dos serviços
  - A entrega da solução deverá ocorrer em até no máximo 30 (trinta) dias corridos a partir da data de assinatura do contrato.
  - A implantação completa da solução deverá ser concluída em até 10 (dez) dias corridos após a entrega do objeto.
  - O(s) equipamento(s) deverão ser entregues e instalados no local indicado pelo departamento de Tecnologia da Informação e Comunicação da Prefeitura Municipal de Sorriso, conforme ordem de fornecimento emitida. A entrega e instalação deverá ser realizada em dias úteis no horário das 07:00 às 11:00 e das 13:00 às 17:00 (horário local).
  - A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
  - O suporte técnico deverá ser de, no mínimo, 3 anos.
- Documentação mínima exigida
  - A Contratada deverá fornecer:
    - Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;
    - Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas.
    - Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
- Formas de transferência de conhecimento
  - A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação direta dos técnicos do Departamento de Tecnologia da Informação e Comunicação da Prefeitura Municipal de Sorriso. Durante a implantação da solução a equipe da Contratada deverá repassar as informações para a equipe responsável da prefeitura apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

9.2. CRITÉRIOS DE ACEITAÇÃO

9.2.1. Para Item 1 – EQUIPAMENTO DE PROTECAO DE REDE – LOCAÇÕA DE SOLUÇÃO DE SEGURANÇA DE REDE APPLIANCE NEXT GENERATION FIREWALL CLUSTER, COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA MÍNIMA DE 36 MESES

- ✓ Apresentar documentação técnica (manuais, catálogos oficiais do fabricante) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto-a-ponto, com indicação de nome do documento e página que comprova o atendimento. Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante, exceto quando explicitamente permitido em algum item específico. Em caso de dúvidas ou divergência na comprovação da especificação técnica, a Prefeitura Municipal de Sorriso poderá solicitar uma amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e

comprovação dos itens pendentes, nas dependências do local designado pela Prefeitura Municipal de Sorriso.

- ✓ Executar o objeto diretamente, sendo vedada a subcontratação, exceções apenas para empresas revendedoras oficiais de fabricantes.
- ✓ O produto será inspecionado no ato da instalação, afim de verificar a conformidade e realizar a inspeção visual da solução. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos usados ou de demonstração.
- ✓ A existência de inspeção não isenta a contratada da responsabilidade pela qualidade do material fornecido.
- ✓ O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

9.2.2. Para Item 2 - SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL:

- ✓ Referente à instalação, o aceite do serviço somente será dado após comprovação da instalação e o efetivo cumprimento de todas as configurações necessárias para funcionamento do equipamento dentro da estrutura da Prefeitura Municipal de Sorriso bem como a migração das regras de firewall existentes.
- ✓ Referente ao treinamento e repasse de conhecimento, o aceite do serviço somente será dado após a apresentação de todos os conteúdos esperados e da resolução de possíveis dúvidas da equipe em treinamento.
- ✓ Caso seja verificada alguma inconformidade na aceitação inicial do objeto, a Contratante informará à Contratada os motivos da não aceitação, devolvendo o(s) bem(ns) para correção.
- ✓ Caberá à Contratada sanar as irregularidades identificadas na instalação, inclusive, substituir equipamentos não aprovados no prazo de 15 (quinze) dias da notificação, às suas expensas, quando fornecidos com problemas, apresentados fora das especificações técnicas estabelecidas, sob pena de incorrer nas sanções legais cabíveis.

9.2.3. Procedimentos de Teste e Inspeção:

- ✓ Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo Departamento de Tecnologia da Informação e Comunicação acompanhados dos fiscais do contrato.
- ✓ Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:
  - Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;
  - Verificar se o equipamento está novo e sem uso;
  - Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;
  - Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;
  - Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);

- Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);

Após, deverá ser conduzida a inspeção através da verificação da conformidade da execução dos serviços em relação aos requisitos exigidos nas especificações técnicas. Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes.

Para esta etapa deve-se observar a seguinte lista de verificação:

- Conectar cabos de alimentação e verificar funcionamento dos equipamentos;
- Conectar cabos de conexões e verificar funcionamentos das portas do equipamento;
- Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS), migração das regras existentes no firewall da contratante);
- Realizar a criação de objetos, de políticas de segurança e regras de firewall;
- Realizar a configuração do serviço DHCP;
- Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Prefeitura Municipal de Sorriso para monitoramento de ativos de rede;
- Realizar a configuração do software de gerenciamento centralizado e armazenamento de logs, e verificar a integração e sincronismo entre o firewall e o software;
- Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
- Testar as seguintes funcionalidades no firewall:
  - Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;
  - Decriptografar tráfego SSL para inspeção de conteúdo;
  - Permitir inspeção em camada 7 (nível de aplicação);
  - Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;
  - Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;
  - Realizar a tradução de endereços IP: NAT (Network Address Translation);
  - Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Prefeitura Municipal de Sorriso remotamente;
  - Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;
  - Deverá ser analisada a performance da solução na infraestrutura da Prefeitura Municipal de Sorriso, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;
  - Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;
  - Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

✓ A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:

- O cumprimento dos prazos e outras obrigações assumidas pela contratada;
- Entrega da documentação exigida;
- Atendimento dos critérios de aceitação;

- Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico;
- A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;
- Durante a vigência do suporte técnico, a fiscalização técnica dos contratos avaliará constantemente a prestação do serviço.
- A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

10. GERENCIAMENTO E DA FISCALIZAÇÃO:

10.1 Secretaria Municipal de Administração:
TITULAR: MEC-UZAID BEZERRA DE SIQUEIRA
SUBSTITUTO: LUCIANO LUIZ OTOWICZ

11. DOS REQUESITOS DA CONTRATANTE

11.1. São direitos e responsabilidades da CONTRATANTE os seguintes:

a) Cumprir fielmente este Contrato, inclusive no que tange aos pagamentos pelos serviços contratados.
b) Permitir o livre acesso dos empregados da empresa CONTRATADA a fim de que possam executar suas tarefas;
c) Efetivar a satisfação do crédito da CONTRATADA, nos precisos termos dispostos neste instrumento;
d) Prestar quaisquer esclarecimentos que venham a ser formalmente solicitados pela CONTRATADA e pertinente ao objeto do presente pacto;
e) Interromper, incontinenti, os serviços que apresentarem irregularidades em sua prestação, comunicando o fato imediatamente à CONTRATADA, bem como qualquer eventual ocorrência de relevo relacionado com o mesmo.
f) Velar pelo bom andamento do presente contrato, dirimindo dúvidas porventura existentes, através da Secretaria Municipal de Administração/Departamento de TI;
g) A Prefeitura Municipal de Sorriso reserva-se o direito de não efetuar o pagamento se os dados constantes da Nota Fiscal estiverem em desacordo com os dados da empresa vencedora do certame licitatório;
h) Fornecer e colocar à disposição da CONTRATADA todos os elementos e informações que se fizerem necessários à execução do fornecimento;
i) Proporcionar condições para a boa consecução do objeto deste contrato;
j) Aplicar as penalidades regulamentares e contratuais no caso de inadimplemento das obrigações da CONTRATADA. Notificando a CONTRATADA, por escrito e com antecedência, sobre multas, prazos, penalidades e quaisquer débitos de sua responsabilidade. E em caso de descobrimento após notificação podendo haver encerramento de contrato.
k) Cumprir e fazer cumprir os termos das Leis nº 14.133/2021, do presente instrumento, inclusive no que diz respeito ao equilíbrio econômico-financeiro durante a execução do contrato;
l) Efetuar os pagamentos devidos à CONTRATADA no prazo estipulado no contrato depois do recebimento das notas fiscais, já devidamente atestadas pelo servidor responsável pela fiscalização;
m) Modificar o contrato, unilateralmente, para melhor adequação às finalidades de interesse público respeitando os direitos da CONTRATADA;

12. DAS SANÇÕES/PENALIDADES:

12.1. Conforme disposto na Lei Federal n° 14.133/2024 e suas alterações (Institui normas para Licitações e Contratos da Administração).

13. DAS DISPOSIÇÕES GERAIS:

13.1. É vedado caucionar o contrato decorrente do presente instrumento para qualquer operação financeira, sem prévia e expressa autorização da Administração.
13.2. A licitante vencedora deverá prestar os serviços quando solicitados, de acordo com as necessidades do Prefeitura de Sorriso, em estrita conformidade com disposições e especificações deste termo e pelo preço registrado.
13.3. Correrão por conta da CONTRATADA todas as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes da entrega e da própria aquisição dos produtos, correndo a cargo da CONTRATANTE absolutamente os valores referentes ao efetivo fornecimento do objeto ao preço cotado na proposta da CONTRATADA.
13.4. Os preços ofertados devem ser expressos em real, unitários e totais e devem compreender todos os custos e despesas que, direta ou indiretamente decorra do cumprimento pleno e integral do objeto deste edital, tais como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, e quaisquer outras taxas, custos ou emolumentos que incidam ou venham a incidir sobre os produtos.

14. DOS REQUISITOS PARA PARTICIPAÇÃO:

1 14.1. HABILITAÇÃO JURIDICA: Conforme disposto na Lei Federal n° 14.133/2021 e suas alterações (Institui normas para Licitações e Contratos da Administração).
14.2. REGULARIDADE FISCAL: Conforme disposto na Lei Federal n° 14.133/2021 e suas alterações (Institui normas para Licitações e Contratos da Administração).
14.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA: Conforme disposto na Lei Federal n° 14.133/2021 e suas alterações (Institui normas para Licitações e Contratos da Administração).
14.4. QUALIFICAÇÃO TÉCNICA PESSOA JURIDICA: Conforme disposto na Lei Federal n° 14.133/2021 e suas alterações (Institui normas para Licitações e Contratos da Administração).

Sorriso – MT, 05 de junho de 2024.

Equipe Técnica
KLAITON DE ARAUJO MONTEIRO
Matrícula: 4203

Equipe Técnica
SARAH FRANCIELI ROLDO
Matrícula: 12762

Equipe de Apoio
MARCIEL DE SOUZA VIANA
Matrícula: 5925

SECRETARIO MUNICIPAL DE ADMINISTRAÇÃO
Bruno Eduardo Pecinelli Delgado

ANEXO I – ESPECIFICAÇÃO DOS ITENS

ITEM	CÓDIGO ÁGILI	COD TCE	NAT DESP	DESCRIÇÃO	UND	MÉDIA	QTD	TOTAL
1	858358	373201-0	339040	SERVICO DE LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA - DO TIPO SERVIDOR FIREWALL , COM SUPORTE, BACKUP DE 12 MESSES DE ACESSO, COM TODAS AS LICENÇAS NECESSÁRIAS PARA BOM FUNCIONAMENTO E VIGÊNCIA DE 03 ANOS	MÊS	R$ 32.418,31	36	R$ 1.167.058,98
2	858233	216552-0	339040	SERVIÇO DE INSTALAÇÃO E IMPLANTAÇÃO DE FIREWALL.	UND	R$ 40.085,73	1	R$ 40.085,73
3	858234	404920-9	339040	SERVICO DE TREINAMENTO NA AREA DE INFORMATICA - FIREWALL DE APLICACAO WEB E VULNERABILIDADES WEB,	UND	R$ 9.347,41	1	R$ 9.347,41

				COM CARGA HORARIA DE ATÉ 04 HORAS, INCLUINDO CERTIFICAÇÃO.				
						TOTAL:	R$ 1.216.492,13	

ITEM 1: LOCAÇÃO DE FIREWALL, INCLUINDO TODAS AS LICENÇAS NECESSÁRIOS PARA OPERAÇÃO, SERVIÇO DE ARMAZENAMENTO COM RETENÇÃO DE LOG, SERVIÇO DE SUPORTE DE OPERAÇÃO E MONITORAMENTO INFINITO, SERVIÇO DE ANALISE DE VUNERABILIDADE DE FIREWALL SEMETRAL, TODOS COM DURANÇÃO DE 36 MESES. QUANTIDADE: 01 UNIDADES

- **CARACTERÍSTICAS DO EQUIPAMENTO**
  - SUPORTAR 7.8 MILHÕES DE CONEXÕES SIMULTÂNEAS;
  - SUPORTE A, NO MÍNIMO, 100 MPPS;
  - SUPORTE A, NO MÍNIMO, 500 MIL NOVAS CONEXÕES POR SEGUNDO;
  - SUPORTAR 8.000 CONEXÕES VPN IPSEC CLIENT-TO-SERVER, SENDO DESTAS 4.000 CONEXÕES SIMULTANEAMENTE;
  - SUPORTAR 4.000 ACESSOS DE USUÁRIOS SIMULTÂNEOS;
  - CAPACIDADE DE PROCESSAMENTO DE FIREWALL DE 135 GBPS;
  - CAPACIDADE DE PROCESSAMENTO DE IPS DE 14 GBPS;
  - CAPACIDADE DE PROCESSAMENTO DE VPN IPSEC DE 50 GBPS;
  - CAPACIDADE DE PROCESSAMENTO DE VPN SSL DE 04 GBPS;
  - ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, ATÉ 4.000 CLIENTES DE VPN SSL SIMULTÂNEOS;
  - POSSUIR AO MENOS 16 INTERFACES 1GBPS RJ45;
  - POSSUIR AO MENOS 08 INTERFACES 1GBPS SFP;
  - POSSUIR AO MENOS 04 INTERFACES 10GBPS SFP+;
  - POSSUIR AO MENOS 04 INTERFACES 25GBPS SFP28;
  - POSSUIR AO MENOS 01 INTERFACE 1GBPS RJ45 DEDICADA À GERENCIAMENTO;
  - POSSUIR AO MENOS 01 INTERFACE SERIAL DE CONSOLE;
  - POSSUIR AO MENOS 02 PORTAS USB;
  - POSSUIR AO MENOS 01 INTERFACES 1GBPS RJ45 DEDICADAS À HA (ALTA DISPONIBILIDADE);

- **REQUISITOS MÍNIMOS DE FUNCIONALIDADE**
  - **CARACTERÍSTICAS GERAIS**
    - O EQUIPAMENTO DEVE SER NOVO E SEM HISTÓRICO DE USO ANTERIOR;
    - O EQUIPAMENTO DEVE ESTAR EM PRODUÇÃO ATUAL, OU SEJA, NÃO PODEM SER OBSOLETOS OU DESCONTINUADOS.
    - É FUNDAMENTAL QUE OS DISPOSITIVOS NÃO ESTEJAM PRÓXIMOS DA DATA DE FIM DE SUPORTE OFICIAL DO FABRICANTE, GARANTINDO SUA VIABILIDADE E SUPORTE A LONGO PRAZO.
    - A CONTRATADA DEVERÁ FORNECER, INSTALAR, CONFIGURAR E MANTER, EM REGIME DE LOCAÇÃO, EQUIPAMENTO(S) PARA PROTEÇÃO POR PERÍMETRO (FIREWALL / UTM) PARA PROTEÇÃO DO ACESSO AO CANAL DE COMUNICAÇÃO DESCRITO NESTE EDITAL;
    - NA PROPOSTA DEVERÁ SER FORNECIDO A MARCA E O MODELO DO(S) EQUIPAMENTO(S) PARA FINS DE IDENTIFICAÇÃO DAS FUNCIONALIDADES;
    - SEMPRE QUE REQUERIDO PELA CONTRATANTE, A CONTRATADA DEVERÁ APRESENTAR DECLARAÇÃO INFORMANDO QUE ELA É PARCEIRA DO FABRICANTE DA SOLUÇÃO OFERTADA E QUE POSSUI CAPACIDADE TÉCNICA E OPERACIONAL PARA EXECUÇÃO DO OBJETO DESTE TERMO DE

REFERÊNCIA, BEM COMO A REALIZAR OS SERVIÇOS DESCRITOS NO PRESENTE EDITAL;

- DEVE SER DISPONIBILIZADO NA FORMA DE NEXT GENERATION FIREWALL (NGFW) OU UNIFIED THREAT MANAGEMENT (UTM);
- IDENTIFICAR O USO DE TÁTICAS EVASIVAS, OU SEJA, DEVE TER A CAPACIDADE DE VISUALIZAR E CONTROLAR AS APLICAÇÕES E OS ATAQUES QUE UTILIZAM TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS, TAIS COMO SKYPE E UTILIZAÇÃO DA REDE TOR;
- PARA TRÁFEGO CRIPTOGRAFADO SSL, DEVE DESCRIPTOGRAFAR PACOTES A FIM DE POSSIBILITAR A LEITURA DE PAYLOAD PARA CHECAGEM DE ASSINATURAS DE APLICAÇÕES CONHECIDAS PELO FABRICANTE;
- 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. A DECODIFICAÇÃO DE PROTOCOLO TAMBÉM DEVE IDENTIFICAR FUNCIONALIDADES ESPECIFICAS DENTRO DE UMA APLICAÇÃO;
- IDENTIFICAR O USO DE TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS;
- SER DISPONIBILIZADO NA FORMA DE APPLIANCE DE HARDWARE, COM RECURSO DE ALTA DISPONIBILIDADE EM MODO ATIVO-ATIVO OU ATIVO-PASSIVO;
- A CONTRATADA DEVERÁ FORNECER TODOS OS CABOS DE ALIMENTAÇÃO, CABOS DE CONSOLE E MÍDIAS, BEM COMO TODOS OS ACESSÓRIOS NECESSÁRIOS PARA A INSTALAÇÃO DO(S) EQUIPAMENTO(S), EM CONFORMIDADE COM AS RECOMENDAÇÕES DO FABRICANTE E PADRÕES INTERNACIONAIS VIGENTES;
- POSSUIR ALIMENTAÇÃO ELÉTRICA A PARTIR DE NO MÍNIMO 2 (DUAS) FONTES INDEPENDENTES E REDUNDANTES, CAPAZES DE OPERAR ENTRE 110-240VAC, 60 HZ;
- A FONTE FORNECIDA DEVE SUPORTAR A OPERAÇÃO DA UNIDADE COM TODOS OS MÓDULOS DE INTERFACE ATIVOS;
- PERMITIR QUE SEJAM LIGADOS NO MÍNIMO 2 LINKS DE INTERNET DE DIFERENTES OPERADORAS;
- PARA GARANTIR MAIOR SEGURANÇA, NÃO SERÃO ACEITOS COMPUTADORES COM INSTALAÇÃO DE SISTEMAS OPERACIONAIS TRADICIONAIS DO MERCADO, TAIS COMO MICROSOFT WINDOWS, FREEBSD, SOLARIS, AIX OU GNU/LINUX;
- 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;
- DEVERÁ SER FORNECIDO DOCUMENTAÇÃO TÉCNICA DO(S) EQUIPAMENTO(S) PROPOSTO, COMTEMPLANDO MANUAL DE USUÁRIO DE UTILIZAÇÃO DO(S) EQUIPAMENTO(S), PODENDO SER EM IDIOMA PORTUGUÊS E/OU INGLÊS;
- DEVERÃO SER FORNECIDAS AS LICENÇAS PARA TODAS AS FUNCIONALIDADES SOLICITADAS NESTE TERMO DE REFERÊNCIA, PELO PERÍODO DE VALIDADE DO CONTRATO;
- A PLATAFORMA DE SEGURANÇA DEVERÁ POSSUIR AS FUNCIONALIDADES:
  - FIREWALL;
  - TRAFFIC SHAPPING E QOS;
  - GATEWAY ANTIVÍRUS, ANTI-SPAM, ANTI-BOT;
  - CONTROLE DE APLICAÇÕES WEB E FILTRO DE CONTEÚDO WEB;

- PROXY WEB TRANSPARANTE/EXPLICÍTO E PROXY REVERSO;
- IPS (SISTEMA DE PREVENÇÃO DE INTRUSOS);
- VPN IPSEC E VPN SSL;
- CONTROLE PARA IDENTIFICAÇÃO DE USUÁRIOS;
- PREVENÇÃO DE AMEAÇAS DO TIPO “0-DAY”

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE FIREWALL:
  - CONTROLE DE ACESSO ATRAVÉS DE REGRAS BASEADAS EM USUÁRIO, GRUPO DE USUÁRIOS, ENDEREÇOS IP, FQDN, HORÁRIO, PROTOCOLO E APLICAÇÃO;
  - CRIAÇÃO DE OBJETOS E AGRUPAMENTO DE OBJETOS DE USUÁRIOS, REDES, PROTOCOLOS E SERVIÇOS PARA FACILITAR A CRIAÇÃO DE REGRAS;
  - FUNCIONAMENTO EM MODO ROUTER, PROXY EXPLÍCITO E/OU VLAN-TAGGED;
  - DEVERÁ PERMITIR O CONTROLE DE ACESSO POR SUB-REDE;
  - SUPORTE A TAGS DE VLAN (802.1Q);
  - SUPORTAR O PROTOCOLO 802.1AX OU 802.3AD (LACP-LINK AGGREGATION CONTROL PROTOCOL);
  - DEVER POSSUIR RECURSO DE DEPURAÇÃO DE PACOTES ENVIADO/RECEBIDOS, SIMILAR AO COMANDO TCPDUMP;
  - INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA AUTENTICAÇÃO DE USUÁRIOS;
  - DEVERÁ SUPORTAR SINGLE-SIGN-ON PARA MICROSOFT ACTIVE DIRECTORY;
  - CONTROLE DE ACESSO À INTERNET POR PERÍODOS DO DIA (HORÁRIOS E DIA DA SEMANA);
  - CONTROLE DE ACESSO À INTERNET POR DOMÍNIO (EXEMPLO: SERPRO.GOV.BR E GOV.BR);
  - SUPORTE PBR - POLICY BASED ROUTING;
  - FILTRO DE PACOTES SEM CONTROLE DE ESTADO “STATELESS” PARA VERIFICAÇÃO EM CAMADA 2;
  - CRIAÇÃO DE SERVIÇOS POR PORTA OU CONJUNTO DE PORTAS DOS PROTOCOLOS TCP E UDP;
  - ABERTURA DE NOVAS PORTAS POR FLUXO DE DADOS PARA SERVIÇOS QUE REQUEREM PORTAS DINÂMICAS;
  - PROVER MECANISMO CONTRA ATAQUES DE FALSIFICAÇÃO DE ENDEREÇOS (ANTI-SPOOFING);
  - SUPORTE A SFLOW OU NETFLOW;
  - DETECÇÃO DE PROGRAMAS DE COMPARTILHAMENTO DE ARQUIVOS (PEER-TO-PEER) E DE MENSAGENS INSTANTÂNEAS;
  - POSSIBILITAR CRIAÇÃO DE REGRAS DE FIREWALL ESPECÍFICAS PARA TIPOS DE DISPOSITIVOS IDENTIFICADOS AUTOMATICAMENTE (TABLETS, CELULARES E PCS);
  - SUPORTAR CERTIFICADOS X.509, SCEP, CERTIFICATE SIGNING REQUEST (CSR) E OCSP;
  - SUPORTAR SIP/H.323/SCCP NAT TRAVERSAL;
  - RECURSO PARA TRADUÇÃO DE ENDEREÇOS IP: NAT (NETWORK ADDRESS TRANSLATION) ESTÁTICO E DINÂMICO;
  - DEVE SUPORTAR TRADUÇÃO DE PORTA (PAT);
  - SUPORTE A ROTEAMENTO ESTÁTICO E DINÂMICO: RIP V1, RIP V2, OSPF E BGP;
  - DEVE POSSUIR SUPORTE A JUMBO FRAMES;
  - SUPORTAR OTIMIZAÇÃO DO TRÁFEGO ENTRE DOIS EQUIPAMENTOS;
  - DEVE SUPORTAR MODO SNIFFER, PARA INSPEÇÃO VIA PORTA ESPELHADA DO TRÁFEGO DE DADOS DA REDE;

- CONEXÃO CRIPTOGRAFADA ENTRE ESTAÇÃO DE GERENCIAMENTO E O APPLIANCE, TANTO EM INTERFACE GRÁFICA, QUANTO EM CLI (LINHA DE COMANDO);

- SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/ATIVO: EM LAYER 2 E 3:
  - SER DISPONIBILIZADO NA FORMA DE APPLIANCE DE HARDWARE, COM RECURSO DE ALTA DISPONIBILIDADE EM MODO ATIVO-ATIVO OU ATIVO-PASSIVO;
  - A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: SESSÕES;
  - A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: CONFIGURAÇÕES, INCLUINDO, MAS NÃO LIMITADO AS POLÍTICAS DE FIREWALL, NAT, QOS E OBJETOS DE REDE;
  - A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: ASSOCIAÇÕES DE SEGURANÇA DAS VPNS;
  - A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR:TABELAS FIB;
  - O HA (MODO DE ALTA-DISPONIBILIDADE) DEVE POSSIBILITAR MONITORAÇÃO DE FALHA DE LINK;
  - DEVE POSSUIR SUPORTE A CRIAÇÃO DE SISTEMAS VIRTUAIS NO MESMO APPLIANCE;
  - DEVE ESTAR LICENCIADO E/OU TER INCLUÍDO SEM CUSTO ADICIONAL, NO MÍNIMO, 10 SISTEMAS VIRTUAIS LÓGICOS (CONTEXTOS) POR APPLIANCE;
  - EM ALTA DISPONIBILIDADE, DEVE SER POSSÍVEL O USO DE CLUSTERS VIRTUAIS, SEJA ATIVO-ATIVO PERMITINDO A DISTRIBUIÇÃO DE CARGA ENTRE DIFERENTES CONTEXTOS;

- DEVERÁ ATENDER AOS SEGUINTES REQUISITOS DE GERÊNCIA:
  - A SOLUÇÃO DEVE POSSIBILITAR A COLETA DE ESTATÍSTICAS DE TODO O TRÁFEGO QUE PASSAR PELOS EQUIPAMENTOS DA PLATAFORMA DE SEGURANÇA;
  - DEVE PERMITIR A CRIAÇÃO DE ADMINISTRADORES INDEPENDENTES, PARA CADA UM DOS SISTEMAS VIRTUAIS EXISTENTES, DE MANEIRA A POSSIBILITAR A CRIAÇÃO DE CONTEXTOS VIRTUAIS QUE PODEM SER ADMINISTRADOS POR EQUIPES DISTINTAS;
  - A SOLUÇÃO DEVE SUPORTAR ACESSO VIA SSH E INTERFACE WEB (HTTPS), INCLUINDO, MAS NÃO LIMITADO À EXPORTAR CONFIGURAÇÃO DOS SISTEMAS VIRTUAIS (CONTEXTOS) POR AMBAS INTERFACES;
  - O GERENCIAMENTO WEB DEVE PERMITIR/POSSUIR MONITORAÇÃO DE LOGS, FERRAMENTAS DE INVESTIGAÇÃO DE LOGS E ACESSO CONCORRENTE DE ADMINISTRADORES;
  - DEVE POSSUIR UM MECANISMO DE BUSCA POR COMANDOS OU AUTOCOMPLETE NO GERENCIAMENTO VIA SSH, DE FORMA A FACILITAR A CONFIGURAÇÃO PELO ADMINISTRADOR;
  - DEVE SUPORTAR A CRIAÇÃO DE REGRAS QUE FIQUEM ATIVAS EM HORÁRIO DEFINIDO E SUPORTAR CRIAÇÃO DE REGRAS COM DATA DE EXPIRAÇÃO;
  - DEVE SUPORTAR BACKUP AUTOMÁTICO DAS CONFIGURAÇÕES E ROLLBACK DE CONFIGURAÇÃO PARA A ÚLTIMA CONFIGURAÇÃO SALVA;
  - DEVE PERMITIR A VISUALIZAÇÃO DOS LOGS DE UMA REGRA ESPECIAL EM TEMPO REAL;

- DEVE POSSIBILITAR A INTEGRAÇÃO COM OUTRAS SOLUÇÕES DE SIEM DE MERCADO;
- O CONSOLE DE ADMINISTRAÇÃO DEVE SUPORTAR PELO MENOS INGLÊS, ESPANHOL E PORTUGUÊS DO BRASIL;
- O CONSOLE DEVE SUPORTAR O GERENCIAMENTO DE SWITCHES E PONTOS DE ACESSO WIRELESS PARA MELHORAR O NÍVEL DE SEGURANÇA;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS POR GEOLOCALIZAÇÃO, PERMITINDO O TRÁFEGO DE DETERMINADO PAÍS/PAÍSES SEJAM BLOQUEADOS;
- DEVE POSSIBILITAR A VISUALIZAÇÃO DOS PAÍSES DE ORIGEM E DESTINO NOS LOGS DOS ACESSOS;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE TRAFFIC SHAPING E PRIORIZAÇÃO:
  - CONTROLE E A PRIORIZAÇÃO DO TRÁFEGO, PRIORIZANDO BANDA PARA AS APLICAÇÕES (INBOUND/OUTBOUND) ATRAVÉS DA CLASSIFICAÇÃO DOS PACOTES (SHAPING), CRIAÇÃO DE FILAS DE PRIORIDADE, GERÊNCIA DE CONGESTIONAMENTO E QOS;
  - LIMITAR INDIVIDUALMENTE A BANDA UTILIZADA POR APLICAÇÕES (POR EXEMPLO, PEER-TO-PEER, STREAMING, CHAT, VOIP, WEB, ETC.);
  - IDENTIFICAÇÃO TRANSPARENTE DE USUÁRIOS CADASTRADOS NO MICROSOFT ACTIVE DIRECTORY;
  - DEFINIR A BANDA MÁXIMA E BANDA GARANTIDA PARA UM USUÁRIO, IP, GRUPO DE IPS, PROTOCOLO OU APLICAÇÃO;
  - DEVERÁ SUPORTAR O CONTROLE DE BANDA, TANTO PARA LIMITAR, COMO PARA EXPANDIR, BASEADO EM CRITÉRIOS POR GRUPO DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, OU POR SUB-REDE DE ORIGEM E DESTINO, OU ENDEREÇO IP DE ORIGEM E DESTINO.

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE ANTIVÍRUS, ANTI-SPAM E ANTI-BOT:
  - FUNÇÃO DE ANTIVÍRUS EM TEMPO REAL PARA AMBIENTE DE GATEWAY INTERNET PARA OS SEGUINTES PROTOCOLOS: HTTP, SMTP, IMAP, POP3 E FTP;
  - BLOQUEIO DE MALWARES (ADWARE, SPYWARE, HIJACKERS, KEYLOGGERS, ETC.);
  - PROTEÇÃO CONTRA CONEXÕES A SERVIDORES MASTERS DE CONTROLE DE BOTNET (BOTMASTERS);
  - BLOQUEIO DE DOWNLOAD DE ARQUIVOS POR EXTENSÃO, NOME DO ARQUIVO E TIPOS DE ARQUIVO;
  - PERMITIR O BLOQUEIO DE DOWNLOAD DE ARQUIVOS POR TAMANHO;
  - A SOLUÇÃO DE UTM DEVE TER A CAPACIDADE DE DETECTAR E BLOQUEAR SPYWARE.

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE CONTROLE DE APLICAÇÕES WEB E FILTRO DE CONTEÚDO WEB:
  - O RECURSO DE FILTRO DE CONTEÚDO WEB DEVERÁ ESTAR INTEGRADO NA SOLUÇÃO DE SEGURANÇA;
  - DEVERÁ SUPORTAR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY;
  - IDENTIFICAÇÃO TRANSPARENTE DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY;
  - FILTRO DE CONTEÚDO BASEADO EM CATEGORIAS;
  - DEVERÁ CATEGORIZAR A PÁGINA WEB, TANTO PELA SUA URL, COMO PELO ENDEREÇO IP;

- DISPOR DE PELO MENOS 50 CATEGORIAS PARA CLASSIFICAÇÃO DE SITES WEB;
- DISPOR DE BASE DE DADOS COM, NO MÍNIMO, 200 MILHÕES URLS;
- DEVERÁ SUPORTAR MONITORAMENTO DO TRÁFEGO INTERNET, COM OPÇÃO DE BLOQUEIO DE ACESSO AOS USUÁRIOS;
- DEVERÁ POSSIBILITAR A CRIAÇÃO DE CATEGORIAS PERSONALIZADAS;
- DEVERÁ PERMITIR A RECLASSIFICAÇÃO DE SITES WEB;
- DEVERÁ EFETUAR FILTRAGEM DE CONTEÚDO DE TRÁFEGO WEB DE URLS CONHECIDAS COMO FONTE DE MATERIAL IMPRÓPRIO E/OU CÓDIGOS (PROGRAMAS/SCRIPTS) MALICIOSOS, SEJAM EM APPLETS JAVA, COOKIES, ACTIVEX. DEVERÁ MANTER BASE DE URL PRÓPRIA ATUALIZÁVEL DE ACORDO COM POLÍTICAS DA SOLUÇÃO DE SEGURANÇA;
- BLOQUEIO DE PÁGINAS WEB ATRAVÉS DA CONSTRUÇÃO DE FILTROS ESPECÍFICOS COM MECANISMO DE BUSCA TEXTUAL;
- DEVERÁ PERMITIR A CRIAÇÃO DE LISTAS PERSONALIZADAS DE URLS PERMITIDAS (LISTA BRANCA) E BLOQUEADAS (LISTA NEGRA);
- DEVERÁ EFETUAR ATUALIZAÇÕES REGULARES DO PRODUTO SEM INTERROMPER A EXECUÇÃO DOS SERVIÇOS DE FILTRAGEM DE CONTEÚDO WEB;
- DEVERÁ PERMITIR A CRIAÇÃO DE REGRAS PARA ACESSO/BLOQUEIO POR CATEGORIAS, NO MÍNIMO, POR GRUPOS DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, POR ENDEREÇO IP DE ORIGEM/DESTINO, E POR SUB-REDE DE ORIGEM/DESTINO.
- DEVERÁ POSSUIR A FUNCIONALIDADE DE COTA DE TEMPO DE UTILIZAÇÃO POR CATEGORIA;
- DEVERÁ PERMITIR A MONITORAÇÃO DO TRÁFEGO INTERNET SEM BLOQUEIO DE ACESSO AOS USUÁRIOS;
- DEVERÁ PERMITIR A CRIAÇÃO DE, PELO MENOS, 05 (CINCO) CATEGORIAS PERSONALIZADAS;
- DEVERÁ PERMITIR A RECLASSIFICAÇÃO DE SITES WEB, TANTO POR URL, QUANTO POR ENDEREÇO IP;
- DEVERÁ PROVER TERMO DE RESPONSABILIDADE ON-LINE PARA ACEITE PELO USUÁRIO, A SER APRESENTADO TODA VEZ QUE HOUVER TENTATIVA DE ACESSO A DETERMINADO SERVIÇO PERMITIDO OU BLOQUEADO;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE PROXY WEB TRANSPARANTE/EXPLICÍTO E PROXY REVERSO:
  - DEVERÁ FUNCIONAR EM MODO PROXY EXPLÍCITO PARA HTTP E HTTPS, E EM PROXY TRANSPARENTE PARA HTTP;
  - DEVERÁ PERMITIR CONFIGURAÇÃO DA PORTA DO PROXY EXPLÍCITO;
  - DEVERÁ SUPORTAR A FUNCIONALIDADE ATRAVÉS DE PROXY REVERSO PARA REDIRECIONAMENTO DE URLS DO TIPO HTTP OU HTTPS REDIRECIONANDO PARA O SERVIDOR ESPECÍFICO;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE DETECÇÃO E PREVENÇÃO DE INTRUSÃO (IDS/IPS):
  - DEVERÁ EFETUAR A INSPEÇÃO DE TRÁFEGO POR REGRA BASEADA EM IP ORIGEM/DESTINO, POR PROTOCOLO, OU POR PORTA (TCP/UDP);
  - DEVERÁ POSSUIR BASE DE ASSINATURAS DE IPS COM PELO MENOS 10.000 AMEAÇAS CONHECIDAS;
  - DEVERÁ EFETUAR A ATUALIZAÇÃO AUTOMÁTICA DA BASE DE ASSINATURAS;

- DEVERÁ PERMITIR A CRIAÇÃO DE ASSINATURAS PERSONALIZADAS;
- DEVERÁ PERMITIR A FUNCIONALIDADE DE BLOQUEIO COM AS OPÇÕES: PASS, DROP;
- DEVERÁ POSSUIR CAPACIDADE DE REMONTAGEM DE PACOTES PARA IDENTIFICAÇÃO DE ATAQUES;
- DEVERÁ TER A CAPACIDADE DE ANÁLISE DE TRÁFEGO PARA A DETECÇÃO E BLOQUEIO DE ANOMALIAS, TAIS COMO DENIAL OF SERVICE (DOS);
- DEVERÁ POSSUIR POSSIBILIDADE DE HABILITAR O IPS, PARA ANALISAR NO MÍNIMO, OS PROTOCOLOS PADRÕES DE REDE (SMTP, IMAP, POP, DNS, FTP, SSH , TELNET E RLOGIN, E ICMP);
- DEVE POSSUIR NOTIFICAÇÃO DE DETECÇÃO DE ATAQUES ATRAVÉS DE ALARMES NA CONSOLE DE ADMINISTRAÇÃO E ALERTAS VIA CORREIO ELETRÔNICO.
- DEVERÁ POSSUIR CAPACIDADE DE ANÁLISE DE TRÁFEGO PARA A DETECÇÃO E BLOQUEIO DE ANOMALIAS, COMO DENIAL OF SERVICE (DOS) DO TIPO FLOOD, SCAN, SESSION E SWEEP;
- DEVERÁ POSSUIR ALERTA VIA CORREIO ELETRÔNICO;
- DEVERÁ POSSUIR ALARMES NA CONSOLE DE ADMINISTRAÇÃO;
- DEVERÁ POSSUIR MÉTODOS DE NOTIFICAÇÃO DE DETECÇÃO DE ATAQUES;
- DEVERÁ PROVER A TERMINAÇÃO DE SESSÕES VIA TCP RESETS;
- DEVERÁ ARMAZENAR OS LOGS DE SESSÕES;
- DEVERÁ MITIGAR OS EFEITOS DOS ATAQUES DE NEGAÇÃO DE SERVIÇOS;
- DEVERÁ POSSUIR FILTROS DE ATAQUES POR ANOMALIAS;
- DEVERÁ PERMITIR FILTROS DE ANOMALIAS DE PROTOCOLOS;
- DEVERÁ PERMITIR FILTROS DE ANOMALIAS DE TRÁFEGO ESTATÍSTICO DE: FLOODING, SCAN, SOURCE E DESTINATION SESSION LIMIT;
- DEVERÁ SUPORTAR VERIFICAÇÃO DE ATAQUE NA CAMADA DE APLICAÇÃO;
- DEVERÁ POSSUIR AS SEGUINTES ESTRATÉGIAS DE BLOQUEIO: PASS, DROP E RESET;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE VPN:
  - SUPORTE A VPNS IPSEC NOS MODOS SITE-TO-SITE, E CLIENT-TO-SITE;
  - SUPORTE AOS ALGORITMOS DE CRIPTOGRAFIA AES, DES, 3DES;
  - POSSIBILITAR MECANISMO DE CRIAÇÃO DE VPNS ENTRE MÁQUINAS WINDOWS SERVER 2016, 2019, WINDOWS 10 E 11, E O DISPOSITIVO, COM CHAVES DE CRIPTOGRAFIA SIMÉTRICAS COM TAMANHO IGUAL OU SUPERIOR A 128 BITS;
  - FUNCIONAR COMO UM PROVEDOR DE VPN PARA CLIENTES, DE MODO A ATRIBUIR AOS CLIENTES ENDEREÇOS IPS DAS REDES INTERNAS, COLOCANDO-OS, VIRTUALMENTE, DENTRO DAS MESMAS;
  - PROVER CLIENTE VPN PARA AS PLATAFORMAS WINDOWS SERVER 2016 E 2019, WINDOWS 11 E 10, MAC OS X QUE PERMITA USO DE CHAVES CRIPTOGRÁFICAS SIMÉTRICAS COM 128 OU MAIS BITS. DEVE ESTAR LICENCIADA PARA TODOS ESSES CLIENTES;
  - A VPN SSL DEVE POSSIBILITAR O ACESSO A TODA INFRAESTRUTURA DA ÁREA CONTRATANTE, DE ACORDO COM A POLÍTICA DE SEGURANÇA;
  - DEVE SUPORTAR AUTO-DISCOVERY VIRTUAL PRIVATE NETWORK (ADVPN);
  - DEVE SUPORTAR AGREGAÇÃO DE TÚNEIS IPSEC;

- DEVERÁ TRABALHAR, NO MÍNIMO, COM OS PROTOCOLOS: IPSEC, SSL E L2TP;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS PARA CONTROLE DE APLICAÇÃO:
  - DEVERÁ PERMITIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY, RECONHECENDO GRUPOS DE USUÁRIOS CADASTRADOS;
  - RECONHECER PELO MENOS 2000 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;
  - RECONHECER PELO MENOS AS SEGUINTES APLICAÇÕES: BITTORRENT, GNUTELLA, SKYPE, FACEBOOK, LINKED-IN, TWITTER, CITRIX, LOGMEIN, TEAMVIEWER, MS-RDP, VNC, GMAIL, YOUTUBE, HTTP-PROXY, HTTP-TUNNEL, FACEBOOK CHAT, GMAIL CHAT, WHATSAPP, 4SHARED, DROPBOX, GOOGLE DRIVE, SKYDRIVE, DB2, MYSQL, ORACLE, ACTIVE DIRECTORY, KERBEROS, LDAP, RADIUS, ITUNES, DHCP, FTP, DNS, WINS, MSRPC, NTP, SNMP, RPC OVER HTTP, GOTOMEETING, WEBEX, EVERNOTE, GOOGLE-DOCS;
  - DEVERÁ POSSUIR, PELO MENOS, 10 CATEGORIAS PARA CLASSIFICAÇÃO DE APLICAÇÕES;
  - DEVERÁ EFETUAR A MONITORAÇÃO DO TRÁFEGO DE APLICAÇÕES, COM OPÇÃO DE BLOQUEIO DE ACESSO DOS USUÁRIOS;
  - DEVERÁ CONTROLAR AS APLICAÇÕES ATRAVÉS DO COMPORTAMENTO DE TRÁFEGO, INDEPENDENTE DO PROTOCOLO E PORTA UTILIZADOS;
  - DEVERÁ PERMITIR IDENTIFICAÇÃO TRANSPARENTE DE USUÁRIOS CADASTRADOS NO MICROSOFT ACTIVE DIRECTORY;
  - DEVERÁ EFETUAR A INSPEÇÃO/BLOQUEIO DE CÓDIGOS MALICIOSOS PARA, NO MÍNIMO, AS CATEGORIAS DE APLICAÇÕES INSTANT MESSAGING E TRANSFERÊNCIA DE ARQUIVOS;
  - DEVERÁ EFETUAR ATUALIZAÇÕES REGULARES DO PRODUTO, DE FORMA QUE SEJA SEM INTERROMPER A EXECUÇÃO DOS SERVIÇOS DA SOLUÇÃO;
  - PERMITIR CRIAÇÃO DE PADRÕES DE APLICAÇÃO MANUALMENTE;
  - PERMITIR A CRIAÇÃO DE REGRAS PARA ACESSO/BLOQUEIO POR CATEGORIAS, NO MÍNIMO, POR GRUPOS DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, POR ENDEREÇO IP DE ORIGEM/DESTINO, E POR SUB-REDE DE ORIGEM/DESTINO.

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE CONTROLE DE IDENTIFICAÇÃO DE USUÁRIOS:
  - DEVE INCLUIR A CAPACIDADE DE CRIAÇÃO DE POLÍTICAS BASEADAS NA VISIBILIDADE E CONTROLE DE QUEM ESTÁ UTILIZANDO QUAIS APLICAÇÕES E URL'S ATRAVÉS DA INTEGRAÇÃO COM SERVIÇOS DE DIRETÓRIO, ACTIVE DIRECTORY, LDAP E RADIUS;
  - DEVE POSSUIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS;
  - DEVE POSSUIR SUPORTE A IDENTIFICAÇÃO DE MÚLTIPLOS USUÁRIOS CONECTADOS EM UM MESMO ENDEREÇO IP EM

AMBIENTES MICROSOFT TERMINAL SERVER, PERMITINDO VISIBILIDADE E CONTROLE GRANULAR;
- DEVERÁ POSSIBILITAR A INTEGRAÇÃO COM ARUBA CLEAR PASS;
- A SOLUÇÃO DEVERÁ SER CAPAZ DE IDENTIFICAR NOME DO USUÁRIO, LOGIN, MAQUINA/COMPUTADOR REGISTRADOS NO MICROSOFT ACTIVE DIRECTORY;
- DEVE SUPORTAR AUTENTICAÇÃO KERBEROS TRANSPARENTE PARA SINGLE SIGN ON;
- NA INTEGRAÇÃO COM O AD, TODOS OS DOMAIN CONTROLLERS EM OPERAÇÃO NA REDE DO CLIENTE DEVEM SER CADASTRADOS DE MANEIRA SIMPLES E SEM UTILIZAÇÃO DE SCRITPS DE COMANDO;

- DEVERÁ ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE PREVENÇÃO DE AMEAÇAS DO TIPO “0-DAY”:
  - A SOLUÇÃO DEVE OFERECER SUPORTE PARA ADICIONAR RECURSOS DE DETECÇÃO DE MALWARE AVANÇADO;
  - A SOLUÇÃO DEVE OFERECER SUPORTE PARA EMULAÇÃO COMPLETA DE SISTEMA PARA DETECTAR MALWARE AVANÇADO DURANTE O TEMPO DA EXECUÇÃO;
  - A SOLUÇÃO DEVE INCLUIR UMA LISTA SUMÁRIO DE INDICADORES DE AMEAÇAS QUE INFORMAM PORQUE O ARQUIVO FOI BLOQUEADO COMO MALWARE.

- DEVE ATENDER, NO MÍNIMO, OS SEGUINTES RECURSOS DE SD-WAN:
  - DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM;
  - DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM E DESTINO;
  - DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR PESO. NESTA OPÇÃO DEVE SER POSSÍVEL DEFINIR O PERCENTUAL DE TRÁFEGO QUE SERÁ ESCOADO POR CADA UM DOS LINKS;
  - DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR CUSTO CONFIGURADO DO LINK;
  - DEVE SUPORTAR O BALANCEAMENTO DE LINKS DE INTERFACES FÍSICAS, SUB-INTERFACES LÓGICAS DE VLAN E TÚNEIS IPSEC;
  - DEVE IMPLEMENTAR BALANCEAMENTO DE LINKS SEM A NECESSIDADE DE CRIAÇÃO DE ZONAS OU USO DE INSTÂNCIAS VIRTUAIS;
  - DEVE GERAR LOG DE EVENTOS QUE REGISTREM ALTERAÇÕES NO ESTADO DOS LINKS DO SDWAN, MONITORADOS PELA CHECAGEM DE SAÚDE.
  - DEVE SUPORTAR A CONFIGURAÇÃO DE NÍVEL MÍNIMO DE QUALIDADE (LATÊNCIA, JITTER E PERDA DE PACOTES) PARA QUE DETERMINADO LINK SEJA ESCOLHIDO PELO SD-WAN;

- DEVERÁ POSSUIR AS SEGUINTES CERTIFICAÇÕES:
  - CERTIFICAÇÃO WI-FI ALLIANCE;
  - CERTIFICAÇÃO ICSA PARA FIREWALL;
  - CERTIFICAÇÃO ICSA PARA VPN SSL;
  - CERTIFICAÇÃO ICSA PARA VPN IPSEC;
  - CERTIFICAÇÃO ICSA PARA IPS;

- **REQUISITOS MÍNIMOS DO SERVIÇO**
  - **CARACTERÍSTICAS GERAIS DA PRESTAÇÃO DE SERVIÇO PELA EMPRESA CONTRATADA**
    - GARANTIR PERFORMANCE, ATUALIZAÇÕES AUTOMÁTICAS DAS APLICAÇÕES DE SEGURANÇA.

- FORNECER UM PORTAL PARA ABERTURA DE CHAMADOS QUANDO OCORRER PROBLEMAS TÉCNICOS OU SOLICITAÇÕES DE SERVIÇO.
- FORNECER UM TELEFONE PARA ABERTURA DE CHAMADOS QUANDO OCORRER PROBLEMAS TÉCNICOS OU SOLICITAÇÕES DE SERVIÇO.
- OS ATENDIMENTOS PODERÃO SER REMOTOS OU PRESENCIAIS OCORRENDO EM REGIME 24X7 E RESPEITANDO OS SEGUINTES ACORDOS DE NÍVEIS DE SERVIÇO:

SLA	IMPACTO
1 - CRÍTICO	O SERVIÇO ENCONTRA-SE INOPERANTE OU EFETIVAMENTE INUTILIZÁVEL DEVIDO A UM PROBLEMA.
2 - ALTO	O SERVIÇO ESTÁ NO AR E OPERANDO, PORÉM, O PROBLEMA CAUSA IMPACTO SIGNIFICATIVO, ESTANDO COM DESEMPENHO SIGNIFICATIVAMENTE REDUZIDO OU FUNCIONALIDADES CONSIDERADAS IMPORTANTES DESATIVADAS.
3 - MÉDIO	IMPACTO LIMITADO OU INSIGNIFICANTE. É IMPORTANTE PARA A PRODUTIVIDADE A LONGO PRAZO, MAS NÃO CAUSA INTERRUPÇÃO DO SERVIÇO.
4 - BAIXO	SERVIÇOS USADOS ESPORADICAMENTE, COM BAIXO IMPACTO.

SLA	TEMPO DE INÍCIO DE ATENDIMENTO	TEMPO DE RESOLUÇÃO
1 - CRÍTICO	2 HORAS	6 HORAS
2 - ALTO	4 HORAS	24 HORAS
3 - MÉDIO	16 HORAS	72 HORAS
4 - BAIXO	32 HORAS	15 DIAS

- A SUBSTITUIÇÃO DO(S) EQUIPAMENTO(S) PELA CONTRATADA, CASO HAJA MAL FUNCIONAMENTO POR OUTRO EQUIPAMENTO COMPATÍVEL COM A SOLUÇÃO JÁ EXISTENTE, EM ATÉ 01(UM) DIA ÚTIL, CONTADOS A PARTIR DA IDENTIFICAÇÃO DO PROBLEMA.

- A CONTRATADA DEVERÁ DISPONIBILIZAR FERRAMENTA DE ARMAZENAMENTO E CENTRALIZAÇÃO DE LOG COM AS SEGUINTES CARACTERÍSTICAS:
  - A SOLUÇÃO DEVE SER BASEADA EM MÁQUINA VIRTUAL OU APPLIANCE FÍSICO DO MESMO FABRICANTE DA SOLUÇÃO DE NGFW, E TER COMO OBJETIVO RECEBER OS LOGS DE TODOS OS EQUIPAMENTOS PARA CONSOLIDAR UMA VISÃO DE NOC E SOC A PARTIR DE UMA CONSOLE ÚNICA DE ADMINISTRAÇÃO;
  - DEVE ESTAR DEVIDAMENTE LICENCIADA PARA:
    - SUPORTAR A COLETA DE, NO MÍNIMO, 05 GB DE LOGS DIÁRIOS;
    - A SOLUÇÃO PODERÁ SER HOSPEDADA NAS DEPENDÊNCIAS DA CONTRATADA OU DO CONTRATANTE, CONTANTO QUE ATENDA AOS REQUISITOS SOLICITADOS;
    - NÃO DEVERÁ EXISTIR LIMITE PARA O NÚMERO DE VCPUS NO APPLIANCE VIRTUAL;
    - NÃO DEVERÁ EXISTIR LIMITE PARA A EXPANSÃO DA MEMÓRIA RAM NO APPLIANCE VIRTUAL;
  - DEVE GARANTIR A GERAÇÃO DE RELATÓRIOS COM MAPAS GEOGRÁFICOS OU MODO TABELA, GERADOS EM TEMPO REAL, PARA A VISUALIZAÇÃO DE ORIGENS E DESTINOS DO TRÁFEGO;
  - DEVE POSSUIR MECANISMO PARA QUE LOGS ANTIGOS SEJAM REMOVIDOS AUTOMATICAMENTE, APÓS ESTAREM CONSOLIDADOS NA SOLUÇÃO DE GUARDA E ANÁLISE DE LOGS E RELATORIA;

- DEVE PERMITIR A EXTRAÇÃO DE RELATÓRIOS;
- DEVE GARANTIR A EXPORTAÇÃO DOS LOGS;
- DEVE POSSUIR RELATÓRIOS PRÉ-DEFINIDOS;
- DEVE POSSIBILITAR A DUPLICAÇÃO DE RELATÓRIOS E GRÁFICOS EXISTENTES PARA EDIÇÃO DOS MESMOS LOGO EM SEGUIDA;
- DEVE POSSUIR A CAPACIDADE DE PERSONALIZAÇÃO DE CAPAS PARA OS RELATÓRIOS;
- DEVE PERMITIR A GERAÇÃO DE RELATÓRIOS DE LOGS DE TRÁFEGO DE DADOS;
- DEVE POSSUIR A CAPACIDADE DE PERSONALIZAÇÃO DE GRÁFICOS COMO BARRA, LINHA, TABELA E PIZZA, PARA INSERÇÃO AOS RELATÓRIOS;
- DEVE POSSUIR MECANISMO PARA EXIBIR DE FORMA DETALHADA INFORMAÇÕES COMPLEMENTARES NOS RELATÓRIOS EM TEMPO REAL;
- DEVER SER POSSÍVEL FAZER DOWNLOAD DOS ARQUIVOS DE LOGS RECEBIDOS;
- DEVE POSSIBILITAR O ENVIO DE MANEIRA AUTOMÁTICA DE RELATÓRIOS POR E-MAIL;
- DEVE PERMITIR CUSTOMIZAÇÃO DE QUAISQUER RELATÓRIOS FORNECIDOS PELA SOLUÇÃO, EXCLUSIVAMENTE A CRITÉRIO DA CONTRATANTE, ADAPTANDO-O ÀS SUAS NECESSIDADES;
- DEVE TER A CAPACIDADE DE DEFINIR FILTROS NOS RELATÓRIOS;
- DEVE SER POSSÍVEL RECEBER LOGS DAS POLÍTICAS DE FIREWALL EM MODO DE APRENDIZADO APLICADAS DIRETAMENTE NOS NGFWS.
- DEVE SER CAPAZ DE DEFINIR O LAYOUT DO RELATÓRIO, INCLUIR GRÁFICOS, INSERIR TEXTOS E IMAGENS, ALINHAMENTO, QUEBRAS DE PÁGINAS, DEFINIR FONTES, CORES, ENTRE OUTROS;
- DEVE GARANTIR A CAPACIDADE DE CRIAR CONSULTAS SQL OU SEMELHANTE PARA USO NOS GRÁFICOS E TABELAS DE RELATÓRIOS;
- DEVE SUPORTAR AUTENTICAÇÃO DE ADMINISTRADORES EM BASE LOCAL E DE MODO REMOTO POR MEIO DE RADIUS, LDAP, TACACS+ E PKI.
- DEVE DISPOR DE RELATÓRIOS CONTEMPLANDO INFORMAÇÕES DO AMBIENTE, DOS EVENTOS DE SEGURANÇA E INCIDENTES, DAS AMEAÇAS, DO USO DA NAVEGAÇÃO WEB, DE IPS, DA UTILIZAÇÃO DA REDE, ENTRE OUTROS.
- DEVE DISPONIBILIZAR UMA AVALIAÇÃO CONSOLIDADA DAS AMEAÇAS CIBERNÉTICAS.
- DEVE DISPOR DE PAINEL GRÁFICO PARA ANÁLISE DAS AMEAÇAS DETECTADAS ENGLOBANDO CONTROLE DE APLICAÇÃO, IPS, FILTRO WEB E ANTIVÍRUS, DEMONSTRANDO AINDA OS PRINCIPAIS DESTINOS, PRINCIPAIS AMEAÇAS, PRINCIPAIS INCIDENTES DE VÍRUS, ENTRE OUTROS.
- A SOLUÇÃO DEVE TER CAPACIDADE DE COLETAR E CORRELACIONAR DADOS DE SEGURANÇA DE VÁRIAS FONTES, INCLUINDO FIREWALLS, ENDPOINTS E OUTROS DISPOSITIVOS DE SEGURANÇA.
- A SOLUÇÃO DEVE TER UMA INTERFACE FÁCIL DE USAR PARA A CRIAÇÃO DE PLAYBOOKS PERSONALIZADOS QUE AUTOMATIZAM PROCESSOS DE RESPOSTA A INCIDENTES E SIMPLIFICAM OS ESFORÇOS DE INVESTIGAÇÃO.
- A SOLUÇÃO DEVE SER CAPAZ DE FORNECER INSIGHTS VALIOSOS SOBRE TENDÊNCIAS E PADRÕES DE SEGURANÇA PARA PERMITIR QUE AS ORGANIZAÇÕES IDENTIFIQUEM ÁREAS DE FRAQUEZA EM

SUAS DEFESAS DE SEGURANÇA E TOMEM MEDIDAS PROATIVAS PARA ABORDÁ-LAS.

- A SOLUÇÃO DEVE TER A CAPACIDADE DE INTEGRAR-SE A OUTROS SISTEMAS DE SEGURANÇA PARA FORNECER UMA VISÃO ABRANGENTE E UNIFICADA DOS DADOS DE SEGURANÇA.
- A SOLUÇÃO DEVE TER A CAPACIDADE DE GERAR ALERTAS EM TEMPO REAL PARA PERMITIR QUE AS EQUIPES DE SEGURANÇA RESPONDAM RAPIDAMENTE A AMEAÇAS DE SEGURANÇA.
- A SOLUÇÃO DEVE TER RECURSOS DE RELATÓRIOS AVANÇADOS PARA PERMITIR QUE AS ORGANIZAÇÕES ACOMPANHEM O DESEMPENHO DE SUAS DEFESAS DE SEGURANÇA E IDENTIFIQUEM ÁREAS DE MELHORIA.
- ATRAVÉS DA ANÁLISE DE TRÁFEGO DE REDE, WEB E DNS, DEVE SUPORTAR A VERIFICAÇÃO DE MÁQUINAS POTENCIALMENTE COMPROMETIDAS OU USUÁRIOS COM USO DE REDE SUSPEITO;
- DEVE REALIZAR AGREGAÇÃO VIA PONTUAÇÃO, PARA GERAÇÃO DE UM VEREDITO SOBRE MÁQUINAS COMPROMETIDAS NA REDE E ATIVIDADES SUSPEITAS;
- DEVE UTILIZAR TÉCNICAS DE MACHINE LEARNING PARA A CAPTURA DE ÍNDICES DE COMPROMETIMENTO, ATRAVÉS DE URLS, DOMÍNIOS E ENDEREÇOS IPS MALICIOSOS;
- DEVE POSSUIR UM PAINEL COM AS INFORMAÇÕES DE MÁQUINAS COMPROMETIDAS INDICANDO INFORMAÇÕES DE ENDEREÇO IP DOS USUÁRIOS, VEREDITO, NÚMERO DE INCIDENTES ETC.;
- A SOLUÇÃO DEVE SER CAPAZ DE RECEBER E INTEGRAR DADOS EM TEMPO REAL DE DIVERSAS FONTES, INCLUINDO FEEDS DE AMEAÇAS EXTERNAS E FONTES INTERNAS DE LOG E TRÁFEGO DE REDE.
- A SOLUÇÃO DEVE SER CAPAZ DE ANALISAR E CORRELACIONAR GRANDES VOLUMES DE DADOS PARA IDENTIFICAR ATIVIDADES SUSPEITAS E INDICADORES DE COMPROMETIMENTO (IOCS[1]).
- A SOLUÇÃO DEVE TER A CAPACIDADE DE ARMAZENAR E CONSULTAR LOGS DE EVENTOS HISTÓRICOS PARA PERMITIR UMA ANÁLISE RETROATIVA QUANDO NOVAS AMEAÇAS FOREM IDENTIFICADAS.
- A SOLUÇÃO DEVE POSSUIR RECURSOS DE DETECÇÃO AUTOMÁTICA DE AMEAÇAS E ALERTAS EM TEMPO REAL PARA PERMITIR QUE AS EQUIPES DE SEGURANÇA RESPONDAM RAPIDAMENTE A POSSÍVEIS AMEAÇAS.
- A SOLUÇÃO DEVE SER CAPAZ DE INTEGRAR-SE COM OUTROS SISTEMAS DE SEGURANÇA PARA FORNECER UMA VISÃO ABRANGENTE E UNIFICADA DOS DADOS DE SEGURANÇA.
- DEVE SER CAPAZ DE VISUALIZAR ALERTAS DE SURTOS E BAIXAR AUTOMATICAMENTE MANIPULADORES DE EVENTOS E RELATÓRIOS RELACIONADOS;
- DEVE PERMITIR O TIME DE RESPOSTA A INCIDENTES IDENTIFICAR SE UM ARTEFATO MALICIOSO DE "ZERO DAY" ENCONTRADO NA REDE FAZ PARTE DE ALGUMA CAMPANHA ESPECÍFICA DE MALWARE, SE FOI VISTO ATÉ O MOMENTO SOMENTE NA REDE DA INSTITUIÇÃO;
- CASO O MALWARE FAÇA PARTE DE ALGUMA CAMPANHA, DEVE SER DETALHADO QUAL O OBJETIVO DELA, TIPOS DE INDÚSTRIA QUE JÁ FORAM ALVO DO MALWARE, COMPORTAMENTO MALICIOSO CONHECIDO SOBRE O MALWARE E QUAIS SÃO OS AUTORES;

[1] Termo utilizado em computação forense para designar artefatos (chaves de registro, arquivos, malwares, IPs etc.) que apontem para uma intrusão. A solução pode investigar os logs coletados em busca de indicadores de comprometimento desenvolvidos pelo time de inteligência do fabricante.

- O SISTEMA DEVE SER CAPAZ DE APRESENTAR AS INFORMAÇÕES SOBRE NOVAS AMEAÇAS E VULNERABILIDADES DE FORMA CLARA E CONCISA, INCLUINDO DETALHES SOBRE O KILL CHAIN
- O SISTEMA DEVE SER CAPAZ DE CRIAR AUTOMATICAMENTE EVENT HANDLERS PARA AUTOMATIZAR A RESPOSTA A NOVAS AMEAÇAS E VULNERABILIDADES, INCLUINDO ATUALIZAÇÕES DE IPS E OUTRAS SOLUÇÕES DE SEGURANÇA.

- INSTALAÇÃO, CONFIGURAÇÃO, MONITORAÇÃO E GESTÃO DO(S) EQUIPAMENTO(S);
  - A INSTALAÇÃO, CONFIGURAÇÃO, PROGRAMAÇÃO E MANUTENÇÃO DO(S) EQUIPAMENTO(S) SÃO DE RESPONSABILIDADE DA CONTRATADA;
  - DEVERÁ SER EXECUTADA PELA EMPRESA CONTRATADA UMA ANÁLISE DA SITUAÇÃO ATUAL E ELABORAR, EM CONJUNTO COM A EQUIPE INTERNA, UM PLANO DE AÇÃO PARA OTIMIZAÇÃO DE RECURSOS, ROTINAS, PROCEDIMENTOS E PROCESSOS PARA O AMBIENTE DE SEGURANÇA DE PERÍMETRO REFERENTE AOS AMBIENTE DO ESCOPO LICITADO. ESSA DOCUMENTAÇÃO DEVERÁ SER ENTREGUE, PELA EMPRESA CONTRATADA, EM FORMATO DIGITAL E EDITÁVEL;
  - OS SERVIÇOS ENVOLVENDO INSTALAÇÃO FÍSICA, MIGRAÇÃO DE REGRAS E CONFIGURAÇÃO INICIAL DA TECNOLOGIA DEVERÃO SER REALIZADAS DE FORMA PRESENCIAL NAS DEPENDÊNCIAS DA CONTRATANTE, SEM QUALQUER ÔNUS FINANCEIRO ADICIONAL PARA A CONTRATANTE;
  - A CONTRATADA DEVERÁ FORNECER TODOS OS CABOS DE ALIMENTAÇÃO, CABOS DE CONSOLE E MÍDIAS, BEM COMO TODOS OS ACESSÓRIOS NECESSÁRIOS PARA A INSTALAÇÃO DO(S) EQUIPAMENTO(S), EM CONFORMIDADE COM AS RECOMENDAÇÕES DO FABRICANTE E PADRÕES INTERNACIONAIS VIGENTES;
  - DEVERÁ SER FORNECIDA AS LICENÇAS PARA FUNCIONAMENTO DO EQUIPAMENTO ATENDENDO AS CARACTERÍSTICAS TÉCNICAS CONFORME ESPECIFICADOS NO EDITAL;
  - TODAS AS CONFIGURAÇÕES DE REGRAS DE POLÍTICAS EXECUTADAS NOS EQUIPAMENTOS SERÃO SEM CUSTOS PARA A CONTRATANTE, PODENDO A CONTRATANTE SOLICITAR ALGUMA CONFIGURAÇÃO ESPECIFICA A QUALQUER MOMENTO DURANTE A VIGÊNCIA DESTE CONTRATO;
  - REALIZAR VISITAS TÉCNICAS PREVENTIVAS NO LOCAL DE INSTALAÇÃO DA SOLUÇÃO (ON-SITE), COM FREQUÊNCIA ANUAL, E COM DURAÇÃO DE PELO MENOS 08 (OITO) HORAS A CADA VISITA, VISANDO ASSEGURAR O MELHOR DESEMPENHO DA SOLUÇÃO.
  - A CONFIGURAÇÃO INICIAL SERÁ FEITA COM BASE NOS PARÂMETROS DE REDE INFORMADOS PELA CONTRATANTE, SENDO QUE AS CONFIGURAÇÕES E A IMPLANTAÇÃO DAS POLÍTICAS SERÃO DEFINIDAS EM CONJUNTO, APÓS A SELEÇÃO DA CONTRATADA;
  - O SISTEMA OPERACIONAL DO(S) EQUIPAMENTO(S) DEVERÁ SER ENTREGUE NA VERSÃO ESTÁVEL MAIS ATUALIZADA. DURANTE A VIGÊNCIA DO CONTRATO, CASO OCORRA NECESSIDADE DE ATUALIZAÇÃO DO SISTEMA OPERACIONAL DO(S) EQUIPAMENTO(S), DEVERÃO SER FORNECIDAS, A CRITÉRIO DA CONTRATADA, SEM QUALQUER ÔNUS ADICIONAL, TODAS AS ATUALIZAÇÕES QUE SE

FIZEREM NECESSÁRIAS AOS SISTEMAS OPERACIONAIS DESSES EQUIPAMENTOS;

- DEVERÁ SER PERMITIDA A SOLICITAÇÃO PARA ALTERAÇÃO DE REGRAS DA SOLUÇÃO DE SEGURANÇA SEM LIMITES QUANTIDADES MENSAIS;
- PARA A CONFIGURAÇÃO DE NOVAS REGRAS/POLÍTICAS DE FIREWALL OU FILTRO DE CONTEÚDO, A CONTRATADA TERÁ O PRAZO DE ATÉ VINTE E QUATRO HORAS PARA APLICAÇÃO;
- OS EQUIPAMENTOS OFERTADOS DEVERÃO POSSUIR CAPACIDADE DE VELOCIDADE E PROCESSAMENTO COMPATÍVEL COM O CIRCUITO DISPONIBILIZADO, E DEVERÃO SER GERENCIÁVEIS PARA UMA ATUAÇÃO MAIS RÁPIDA EM CASO DE CONFIGURAÇÃO E MONITORAMENTO DE FALHA;
- A CONTRATADA DEVERÁ FORNECER ACESSO À CONTRATANTE NA INTERFACE DE GERENCIAMENTO DO EQUIPAMENTO DE SEGURANÇA DE PERÍMETRO, A FIM DE QUE AGILIZAR O GERENCIAMENTO BÁSICO DE REGRAS DE CONTROLE DE CONTEÚDO E REGRAS DE ACESSO (GERENCIAMENTO TOTAL DO EQUIPAMENTO);
- MIGRAÇÃO DE TODAS AS REGRAS DO FIREWALL ATUAL PARA A NOVA SOLUÇÃO;
- A ABERTURA DE CHAMADOS, ASSIM COMO A SOLICITAÇÃO DE SUPORTE REMOTO, SERÁ EFETUADA NO REGIME 24 X 7, OU SEJA, VINTE E QUATRO HORAS POR DIA, SETE DIAS POR SEMANA DE FORMA ILIMITADA.

- A CONTRATADA DEVERÁ REALIZAR BACKUP DAS CONFIGURAÇÕES DE TODOS OS EQUIPAMENTOS, CONTEMPLANDO:
  - A FREQUÊNCIA DO BACKUP DEVE SER DIÁRIA E SEMPRE QUE A CONTRATANTE SOLICITAR;
  - O ARMAZENAMENTO DO BACKUP É DE RESPONSABILIDADE DA CONTRATADA;
  - A CONTRATADA DEVERÁ ARMAZENAR DE FORMA SEGURA, TODOS OS BACKUPS ATÉ O FIM DO CONTRATO;
  - TODOS OS BACKUPS DEVEM ESTAR DISPONÍVEIS PARA QUE A CONTRATANTE TENHA A AUTONOMIA DE RESGATAR SEMPRE QUE NECESSÁRIO;

- A CONTRATADA DEVE ENVIAR MENSALMENTE RELATÓRIO CONTENDO OS PRINCIPAIS INDICADORES DO NGFW COM LEGENDA DESCRITIVA E EXPLICATIVA DE CADA ITEM DO RELATÓRIO, BEM COMO AS RECOMENDAÇÕES COM ORIENTAÇÕES PARA RESOLUÇÃO DE POSSÍVEIS OPORTUNIDADES DE MELHORIAS DETECTADAS E APONTADAS NO RELATÓRIO.

- O RELATÓRIO MENSAL DEVE CONTER NO MÍNIMO AS SEGUINTES INFORMAÇÕES:
  - AMEAÇAS DETECTADAS PELO IPS;
  - AMEAÇAS DETECTADAS PELO ANTIMALWARE;
  - AMEAÇAS DETECTADAS PELO WEBFILTER;
  - TOP 20 - CATEGORIAS DE WEBSITES BLOQUEADOS;
  - WEBSITES COM MAIS BLOQUEIOS DE ACESSO;
  - TOP 20 - TENTATIVAS DE ACESSO A WEBSITES DE PHISHING;
  - AMEAÇAS DETECTADAS PELO APPLICATION CONTROL;

- REDE VIRTUAL PRIVADA (VPN) – QUANTIDADE DE LOGIN, FALHAS DE AUTENTICAÇÃO E UTILIZAÇÃO DE BANDA;
- HISTÓRICO DE CONSUMO DE: PROCESSADOR, MEMÓRIA, DISCO, LOGS, SESSÕES, BANDA;
- EVENTOS DE SISTEMA: TENTATIVAS DE ACESSO SEM SUCESSO, HISTÓRICO DE ACESSO COM SUCESSO; DETALHAMENTO DE MODIFICAÇÕES NAS CONFIGURAÇÕES E REGRAS;

- A CONTRATADA DEVE DISPONIBILIZAR DURANTE A VIGÊNCIA DE CONTRATO, UM MONITORAMENTO ONLINE DO(S) EQUIPAMENTO(S) E DOS LINKS DE COMUNICAÇÃO CONECTADOS DIRETAMENTE NOS EQUIPAMENTOS OBJETO DESSE EDITAL, COM ENVIO DE ALERTAS AUTOMÁTICOS POR E-MAIL E APLICATIVOS DE MENSAGEM INSTANTÂNEA. O MONITORAMENTO DEVE SER CAPAZ DE:
  - DEVE COLETAR O USO DE CPU POR CORE DO PROCESSADOR;
  - DEVE SER CAPAZ DE IDENTIFICAR A QUANTIDADE DE CORE AUTOMATICAMENTE;
  - DEVE IDENTIFICAR A QUANTIDADE TOTAL DE MEMÓRIA;
  - DEVE SER CAPAZ DE IDENTIFICAR O USO DE MEMÓRIA EM PERCENTUAL E EM MEGABYTES;
  - DEVE MONITORAR O CONSUMO DE TODAS AS INTERFACES DE REDE DO(S) EQUIPAMENTO(S), SEM A NECESSIDADE DE CADASTRO MANUAL DE INTERFACES PELO ADMINISTRADOR;
  - COLETAR SERIAL NUMBER DE TODOS OS EQUIPAMENTOS;
  - DEVE COLETAR VERSÃO DE FIRMWARE DO EQUIPAMENTO ;
  - DEVE COLETAR UPTIME DO EQUIPAMENTO+ QUANTIDADE DE TÚNEIS IPSEC ATIVOS;
  - QUANTIDADE DE USUÁRIOS ONLINE ATRAVÉS DA SSL VPN;
  - DEVE IDENTIFICAR A QUANTIDADE DE INTRUSÕES DETECTADAS POR TIPO DE SEVERIDADE (CRÍTICA, ALTA, MÉDIA, BAIXA E INFORMAÇÃO);
  - DEVE COLETAR A VERSÃO DE DATABASE DO IPS NO EQUIPAMENTO;
  - DEVE COLETAR A QUANTIDADE DE SESSÕES IPV4 ATIVAS;
  - DEVE IDENTIFICAR A VERSÃO DE SISTEMA OPERACIONAL;
  - DEVE EXTRAIR OS RESULTADOS DE PERFORMANCE SLA DO SOFTWARE-DEFINED WAN;
  - DEVE IDENTIFICAR A QUANTIDADE DE PACOTES COM ERRO EM CADA INTERFACE;
  - DEVE IDENTIFICAR A VELOCIDADE DE CADA INTERFACE (GIGABIT OU FASTETHERNET);
  - DEVE DETECTAR E EMITIR ALERTAS CASO UMA INTERFACE MUDE O STATUS DE CONECTADA PARA DESCONECTADA E VICE-VERSA;
  - DEVE SER CAPAZ DE EMITIR ALERTAS CASO A VELOCIDADE DE REDE;
  - DEVE SER CAPAZ DE ALERTAR QUANDO A VERSÃO DE FIRMWARE FOR MODIFICADA;
  - DEVE SER CAPAZ DE DISPARAR COMANDOS REMOTO PARA O EQUIPAMENTO NO CASO DE ALGUMA CONDIÇÃO DE INDISPONIBILIDADE DE MÓDULO OU CONDIÇÃO PERSONALIZÁVEL;
  - DEVE PERMITIR O ENVIO DE ALERTA EM ATÉ 02 MINUTOS APÓS O REBOOT DO EQUIPAMENTO;
  - DEVE SER POSSÍVEL O ENVIO DE ALERTAS VIA SMS ;
  - DEVE SER POSSÍVEL O ENVIO DE ALERTAS VIA E-MAIL;
  - DEVE SER POSSÍVEL ENVIO DE DADOS VIA WEBHOOK;

- A CONTRATADA DEVERÁ REALIZAR ANÁLISE DE VULNERABILIDADES SEMESTRAL DE TODOS OS EQUIPAMENTOS NGFW;
  - A ANÁLISE DEVE SER REALIZADA POR UM PROFISSIONAL CERTIFICADO PELO FABRICANTE NA CATEGORIA DE ENGINEER OU EXPERT CONFORME A CLASSIFICAÇÃO DE CADA FABRICANTE E POSSUINDO CERTIFICAÇÃO DE MERCADO COMO CEH, COMPTIA SECURITY+ OU SIMILAR.
  - A CONTRATADA DEVERÁ DISPONIBILIZAR PELO MENOS 02(DOIS) RELATÓRIOS DE ANÁLISE DE VULNERABILIDADES EXTERNA DO FIREWALL, CONTEMPLANDO:
    - ANÁLISE DOS ENDEREÇOS IPS PÚBLICOS DA CONTRATANTE;
    - DEVE SER ENTREGUE O MAPEAMENTO DE PORTAS QUE ESTÃO EM USO E DETECTÁVEIS PELO SCAN;
    - DEVE SER ENTREGUE O DESCRITIVO DE CADA VULNERABILIDADES DESCOBERTAS;
    - AS VULNERABILIDADES DEVEM ESTAR DEVIDAMENTE CATEGORIZADAS E PRIORIZADAS DE ACORDO COM A SEVERIDADE;
    - DEVE CONTER NO RELATÓRIO AS ORIENTAÇÕES DE RESOLUÇÃO DE CADA VULNERABILIDADE;
    - PARA CADA VULNERABILIDADE ENCONTRADA, DEVE SER EXIBIDO DETALHES E EVIDÊNCIAS;
  - AS VULNERABILIDADES IDENTIFICADAS DEVERÃO MOSTRAR SUA SEVERIDADE USANDO NÃO APENAS CONFORME DEFINIDO PELO COMMON VULNERABILITY SCORING SYSTEM (CVSS) V2 E V3, MAS TAMBÉM DEVERÁ CONTEMPLAR DEFINIÇÃO DE SEVERIDADE COM BASE EM MODELO DE INTELIGÊNCIA ARTIFICIAL COMPOSTO DE AO MENOS TRÊS COMPONENTES:
    - MÚLTIPLAS ORIGENS DE DADOS, TAIS COMO: CVSS, INTELIGÊNCIA DE AMEAÇAS, IDADE DAS VULNERABILIDADES, ENTRE OUTRAS;
    - ATUALIZAÇÃO CONTINUA, ONDE O MODELO PODERÁ ATUALIZAR AS SEVERIDADES E PREDIZER AS AMEAÇAS DURANTE ATUALIZAÇÕES REGULARES;
    - TRANSPARÊNCIA DO MODELO, TRAZENDO ASSIM VISIBILIDADE DE QUAIS FATORES LEVADOS EM CONTA, PARA A AVALIAÇÃO DE RISCO, FORAM USADOS;
  - DEVERÁ FORNECER O STATUS DO EXPLOIT DE UMA VULNERABILIDADE COM AO MENOS OS SEGUINTES STATUS:
    - NÃO PROVADO;
    - DISPONÍVEL;
    - FÁCIL ACESSO;
    - USADO ATIVAMENTE;
  - A CONTRATADA DEVE FAZER A CLASSIFICAÇÃO DAS VULNERABILIDADES COM BASE EM SEU RISCO, PERMITINDO QUE AS EQUIPES SE CONCENTREM NAS MAIS CRÍTICAS PRIMEIRO.

- **GARANTIA**
  - A GARANTIA EXIGIDA PARA TODA A SOLUÇÃO SERÁ DE NO MÍNIMO 36 MESES (3 ANOS).

ITEM 2: SERVICO DE TREINAMENTO NA AREA DE INFORMATICA - SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL
QUANTIDADE: 01 UNIDADE

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

- **REUNIÃO DE KICK-OFF**
  - A EMPRESA CONTRATADA, DEVERÁ REALIZAR REUNIÃO COM EQUIPE TÉCNICA DA PREFEITURA E ELABORAR O LEVANTAMENTO DE ITENS NECESSÁRIOS PARA A CRIAÇÃO DO PROJETO PROVISÓRIO DE IMPLANTAÇÃO – PPI. NESTE DOCUMENTO FICARÃO DESCRITAS TODAS AS PARTICULARIDADES DA IMPLANTAÇÃO. A PARTIR DESTE DOCUMENTO A CONTRATADA APRESENTARÁ UM CRONOGRAMA COM DEFINIÇÃO DE DATAS DE ENTREGA DO PROJETO E CADA UMA DE SUAS ETAPAS; TAL REUNIÃO PODE SER PRESENCIAL OU REMOTA;
  - TODAS AS FASES DO PROJETO DEVERÃO SER GUIADAS E GERIDAS POR UM GERENTE DE PROJETOS OU TECNICO CERTIFICADO DA CONTRATADA;
  - O GERENTE DE PROJETOS OU TECNICO CERTIFICADO DA CONTRATADA SERÁ RESPONSÁVEL PELO ACOMPANHAMENTO DIÁRIO DOS TRABALHOS DE IMPLANTAÇÃO E DEVERÁ GERAR O RELATÓRIO DE ATIVIDADES PARA OS RESPONSÁVEIS DA PREFEITURA DE SORRISO – MT. ESTE TRABALHO DEVERÁ INCLUIR ATIVIDADES COMO INÍCIO DO PROJETO, REUNIÕES DE ACOMPANHAMENTO, REUNIÕES DE INÍCIO, CONCLUSÃO DE FASES E CONCLUSÃO DO PROJETO;

- **IMPLANTAÇÃO DE FIREWALL**
  - A IMPLANTAÇÃO DEVE SER REALIZADA DE FORMA PRESENCIAL;
  - A IMPLANTAÇÃO DEVERÁ SER REALIZADA POR PROFISSIONAL CERTIFICADO PELO FABRICANTE NA CATEGORIA DE ENGINEER OU EXPERT CONFORME A CLASSIFICAÇÃO DE CADA FABRICANTE E POSSUINDO CERTIFICAÇÃO DE MERCADO COMO CEH COMPTIA SECURITY+ OU SIMILAR.
  - ATUALIZAÇÃO DE FIRMWARE DO(S) EQUIPAMENTO(S);
  - INTEGRAR A BASE DE USUÁRIOS DO AD DA PREFEITURA AO APPLIANCE PARA EFETUAR CONFIGURAÇÕES DE PERMISSÕES DE ACESSO;
  - CRIAR TODA E QUALQUER REGRA DE NAT NECESSÁRIA;
  - CONFIGURAR FILTRO DE CONTEÚDO DE ACORDO COM DEFINIÇÕES DA PREFEITURA;

- **TESTES OPERACIONAIS E OPERAÇÃO ASSISTIDA**
  - APÓS A CONFIGURAÇÃO, CUSTOMIZAÇÃO E OPERACIONALIZAÇÃO DE TODA SOLUÇÃO, A CONTRATADA DEVE SE COMPROMETER A REALIZAR TODOS OS TESTES OPERACIONAIS PARA GARANTIR O PERFEITO FUNCIONAMENTO DA SOLUÇÃO OFERTADA.
  - A CONTRATADA TERÁ A RESPONSABILIDADE DE AUXILIAR A EQUIPE DA PREFEITURA DE SORRISO A OPERAR O NOVO AMBIENTE. ALÉM DE GUIAR A EQUIPE TÉCNICA DA PREFEITURA DURANTE O TEMPO VIGENTE DA OPERAÇÃO ASSISTIDA
  - OS PROFISSIONAIS DA CONTRATADA DEVERÃO ESTAR À DISPOSIÇÃO PARA QUAISQUER ESCLARECIMENTOS SOBRE A TECNOLOGIA UTILIZADA;
  - TODOS OS TESTES TERÃO O ACOMPANHAMENTO E A APROVAÇÃO DO RESPONSÁVEL DA PREFEITURA.

- **DOCUMENTAÇÃO FINAL**

- APRESENTAÇÃO PARA A EQUIPE DA PREFEITURA DE SORRISO COM A PASSAGEM DE CONHECIMENTO DO PROJETO FINALIZADO, ONDE IRÁ ABRANGER A CONFIGURAÇÃO FÍSICA E LÓGICA E TODAS AS INFORMAÇÕES DAS CONFIGURAÇÕES REALIZADAS NO PROJETO, PERMITINDO QUE A PREFEITURA DE SORRISO TIRE DÚVIDAS A RESPEITO DA SOLUÇÃO IMPLEMENTADA;
- ENTREGA DA DOCUMENTAÇÃO DO PROJETO INSTALADO E SUAS RESPECTIVAS CONFIGURAÇÕES EM MÍDIA ELETRÔNICA EM CD, DVD OU PREFERENCIALMENTE PDF.

ITEM 03: SERVIÇO DE TREINAMENTO PARA O DEPARTAMENTO DE TI
QUANTIDADE: 01 UNIDADE

- **REPASSE DE TECNOLOGIA**
  - A TRANSFERÊNCIA DE CONHECIMENTO COMPREENDERÁ NECESSARIAMENTE OS SEGUINTES TÓPICOS:
    - INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO DO EQUIPAMENTO;
    - APRESENTAÇÃO DO PROJETO;
    - DESCRIÇÃO DA ARQUITETURA DO EQUIPAMENTO;
    - DESCRIÇÃO DO HARDWARE E SOFTWARE DISPONÍVEL;
    - ESTRATÉGIAS DE IMPLEMENTAÇÃO DO(S) EQUIPAMENTO(S);
    - CONFIGURAÇÃO E ADMINISTRAÇÃO DO(S) EQUIPAMENTO(S);
  - A CONTRATADA PODERÁ UTILIZAR OS EQUIPAMENTOS IMPLANTADOS PARA MINISTRAR O TREINAMENTO;
  - O REPASSE DE CONHECIMENTO DEVERÁ SER REALIZADO PARA UMA ÚNICA TURMA DE ATÉ 04 (QUATRO) HORAS;
  - A TRANSFERÊNCIA DE CONHECIMENTO ESTARÁ CENTRADA NA SOLUÇÃO FORNECIDA, PRIVILEGIANDO ATIVIDADES PRÁTICAS QUE PERMITAM UMA MELHOR FIXAÇÃO DO APRENDIZADO, BEM COMO POSSIBILITE A EQUIPE TÉCNICA GERENCIAR A SOLUÇÃO IMPLANTADA;
  - A CONTRATADA DEVERÁ FORNECER, NO INÍCIO DE CADA TÓPICO, APOSTILAS (DIGITAL OU IMPRESSA) QUE ABORDEM TODO O CONTEÚDO PROGRAMÁTICO, AS QUAIS PODERÃO ESTAR NO TODO OU EM PARTE, EM PORTUGUÊS;
  - O INÍCIO DESTA ATIVIDADE, BEM COMO O PERÍODO E HORÁRIO DE REALIZAÇÃO, SERÁ DEFINIDO PELA PREFEITURA EM COMUM ACORDO COM A CONTRATADA;

- **PERFIL DOS PROFISSIONAIS DA CONTRATADA**
  - A CONTRATADA DEVERÁ DISPONIBILIZAR PROFISSIONAIS CERTIFICADOS PELO FABRICANTE DO EQUIPAMENTO OFERTADO NA CATEGORIA ENGINEER OU EXPERT E DEVERÁ APRESENTAR UM ATESTADO DE CAPACIDADE TÉCNICA DE SERVIÇO DE INSTALAÇÃO DE FIREWALL, COMPROVANDO QUE ESTÁ APTA A INSTALAÇÃO DO(S) EQUIPAMENTO(S).

ANEXO II - DOTAÇÕES:

A despesa decorrente do objeto desta licitação ocorrerá à conta de recursos específicos consignados no Orçamento:

ÓRGÃO	DOTAÇÃO	PROJ/ATIVIDADE	ELE DESP	COD RED	VALOR
Secretaria Municipal De Administração	10.001.04.122.0002.2010	Manutenção das Atividades Da SEMAD	339040	526	1.216.492,13
					1.216.492,13