AVISO DE CONTRATAÇÃO DIRETA - SEM DISPUTA

PROCESSO Nº 008/2024

DISPENSA ELETRÔNICA Nº 002/2024

A FEMA – Fundação Educacional do Município de Assis, CNPJ nº 51.501.559/0001-36, em atendimento ao §3º do art. 75 da Lei nº 14.333/2021, torna público para conhecimento dos interessados, o presente aviso da Dispensa de Licitação, que visa a contratação de empresa especializada na prestação de Serviços Gerenciados de Tecnologia da Informação como Serviços Gerenciados de Segurança da Informação, para período de 05 (cinco) meses.

O presente processo obedecerá às disposições do artigo 75, inciso II, da Lei Federal nº 14.133/2021.

As informações referentes aos dados para participação constam no site: https://fema.edu.br/index.php/compraselicitacoes.

Assis, 17 de Abril de 2024.

Hilário Vetore Neto
Diretor Executivo

AVISO DE DISPENSA ELETRÔNICA Nº 002/2024 – SEM DISPUTA

O Diretor Executivo da FEMA, senhor Hilário Vetore Neto, torna público que a FEMA – Fundação Educacional do Município de Assis, sediada na Avenida Getúlio Vargas, nº 1.200 – Vila Nova Santana, Assis-São Paulo, CEP 19807-130, realizará Dispensa eletrônica SEM DISPUTA, com critério de julgamento MENOR PREÇO GLOBAL, nos termos do Art. nº 75, inciso II da Lei 14.133/2021, e de acordo com as condições, critérios e procedimentos estabelecidos neste Regulamento e seus anexos, objetivando obter a melhor proposta, observadas as datas e horários discriminados

1. DO PROCESSAMENTO:

NÚMERO DO PROCESSO:	**008/2024**
INÍCIO DO RECEBIMENTO DAS PROPOSTAS:	**Às 8h00min do dia 18/04/2024**
LIMITE DE ENTREGA DE PROPOSTAS:	**Às 16h59min do dia 23/04/2024**

REFERÊNCIA DE TEMPO: para todas as referências de tempo, será considerado o horário oficial de Brasília – DF.

RECEBIMENTO DAS PROPOSTAS: As propostas deveram ser encaminhadas através do e-mail: materiais@fema.edu.br ou entregue diretamente no setor de compras e licitação, até o prazo limite para entrega.

ENDEREÇO ELETRÔNICO: https://fema.edu.br/index.php/compraselicitacoes.

CRITÉRIO DE JULGAMENTO: MENOR PREÇO GLOBAL.

ESCOLHA DA PROPOSTA: No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado) ou não, a Administração poderá:

a) republicar o presente regulamento com uma nova data;

b) valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas

c) fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

As providências das alíneas acima poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto)

2. DO OBJETO:

2.1. A presente dispensa é a *CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO*, conforme especificações constantes no Anexo I - Termo de Referência, que fica fazendo parte deste aviso de contratação direta.

3. DA PARTICIPAÇÃO NA DISPENSA ELETRÔNICA:

3.1. Poderão participar desta Dispensa todos os interessados que comprovem o atendimento dos requisitos estabelecidos neste instrumento e em seus anexos.

3.2. Não poderão participar da presente licitação:

3.2.1. Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

3.2.2. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ela necessários;

3.2.3. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

3.2.3.1. O impedimento de que trata este item será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.2.4. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

3.2.5. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.2.6. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

2.3. O impedimento de que trata o subitem "3.2.3" do item 3.2 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.4. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os subitens "3.2.1" e "3.2.2" do item 3.2 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.5. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.6. O disposto neste item não impede a licitação ou a contratação de obra ou

serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.7. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei 14.133/2021.

4. DA APRESENTAÇÃO DA PROPOSTA:

4.1. Prazo de validade: 30 (trinta) dias, no mínimo.

4.2. Prazo e forma de pagamento: Será efetuado em até 07 (sete) dias úteis, após a apresentação do relatório mensal juntamente com emissão da Nota fiscal.

4.3. A empresa proponente deverá especificar: Preços global do lote e preço unitário e total de cada item do respectivo lote, expressos em moeda corrente nacional, apurado à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária, incluindo, além do lucro, todas as despesas resultantes de impostos, taxas, tributos, frete e demais encargos, assim como todas as despesas diretas ou indiretas relacionadas com o integral fornecimento do objeto da presente licitação.

4.4. Valor médio estimado do objeto:

	ITEM	DESCRIÇÃO RESUMIDA	QTDE	V.U	V.T
LOTE ÚNICO	**1**	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	5 meses	R$ 5.000,00	R$ 25.000,00
	2	SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO	5 meses	R$ 1.666,67	R$ 8.333,35
	3	SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE INFRAESTRUTURA	5 meses	R$ 2.433,33	R$ 12.166,65
	4	SERVIÇO DE BACKUP EM NUVEM	5 meses	R$ 2.333,33	R$ 11.666,65
			VALOR GLOBAL	**R$ 57.166,65**	

4.5. A contratação será pelo critério de menor preço global do lote.

5. DOCUMENTOS QUE DEVERÃO SER APRESENTADOS COMO CRITÉRIO DE HABILITAÇÃO, PELA EMPRESA QUE APRESENTAR A MELHOR PROPOSTA:

5.1. Para fins de habilitação, deverá o fornecedor comprovar os seguintes requisitos:

5.1.1. HABILITAÇÃO JURÍDICA

5.1.1.1. Registro Comercial, no caso de empresa individual; ou Ato constitutivo (Estatuto ou Contrato Social em vigor), devidamente registrado no Órgão competente, acompanhado de documento comprobatório da eleição dos atuais administradores; ou Inscrição do Ato Constitutivo, no caso de Sociedades Simples, acompanhada de prova de designação da diretoria em exercício.

5.1.2. REGULARIDADE FISCAL E TRABALHISTA

5.1.2.1. Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ), do Ministério da Fazenda.

5.1.2.2. Certidão Conjunta Negativa de Débitos ou Positiva com Efeito de Negativa, relativa a Tributos Federais (inclusive as contribuições sociais) e à Dívida Ativa da União.

5.1.2.3. Certidão de regularidade de débito com a Fazenda Municipal, da sede ou do domicílio do fornecedor, relativa aos tributos incidentes sobre o objeto desta dispensa;

5.1.2.4. Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS).

5.1.2.5. Certidão Negativa ou Positiva de Débitos Trabalhistas com Efeito de Negativa de Débitos Trabalhistas.

5.1.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

5.1.3.1. Certidão negativa de falência e concordata, recuperação judicial ou extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, com data não superior a 180 (cento e oitenta) dias, da data limite para o recebimento das propostas da presente licitação.

5.1.3.2. Nas hipóteses em que a certidão encaminhada for positiva, deve o licitante

apresentar comprovante da homologação/deferimento pelo juízo competente do plano de recuperação judicial/extrajudicial em vigor.

5.1.4. DOCUMENTAÇÃO COMPLEMENTAR

5.1.4.1. Declarações gerais, conforme modelo do Anexo I.

5.1.4.2. Para efeito de concessão de tratamento diferenciado previsto na Lei Complementar nº 123/2006, alterada:

a) Comprovação da condição de Microempresa (ME) ou Empresa de Pequeno Porte (EPP), devendo ser feita com a apresentação de um dos seguintes documentos:

a1) Certidão expedida pela Junta Comercial, caso exerçam atividade comercial, com data inferior a 180 dias;

a2) Documento expedido pelo Registro Civil das Pessoas Jurídicas, caso atuem em outra área que não a comercial, com data inferior a 180 dias.

6. DA CONTRATAÇÃO:

6.1. Após a homologação e adjudicação a contratação será firmada com a emissão de nota(s) de empenho, nos termos do art. 95 da Lei nº 14.133/2021.

6.2. O aceite da Nota de Empenho, emitida à empresa adjudicada, implica no reconhecimento de que:

a) referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133/2021;

b) a contratada se vincula à sua proposta e às previsões contidas no regulamento de Contratação Direta e seus anexos;

c) a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133/2021 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

7. EXECUÇÃO CONTRATUAL:

7.1. Condições Gerais

7.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021, e cada parte responderá

pelas consequências de sua inexecução total ou parcial.

7.1.2. Os serviços contratados deverão funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana durante todo o período da vigência do contrato.

7.1.3. O regime de execução será o de empreitada por preço global.

7.1.4. As comunicações entre a FEMA e a contratada devem ser realizadas, preferencialmente, por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.1.4.1. A contratada deverá informar e-mail e número de telefone móvel com acesso ao aplicativo WhatsApp para recebimento de comunicações escritas relacionadas ao contrato.

7.2. Fiscalização e acompanhamento da execução

7.2.1. A execução das contratações será fiscalizada e acompanhada por representantes da FEMA.

7.2.1.1. A fiscalização será realizada pelo CEPEIN, que atuará em conformidade com as atribuições indicadas neste instrumento.

7.3. Obrigações da FEMA

7.3.1. São obrigações gerais:

a) emitir Nota(s) de Empenho;

b) proporcionar as condições indispensáveis à execução do objeto, prestando informações e esclarecimentos pertinentes que venham a ser solicitados por parte da contratada.

c) fiscalizar a execução da contratação em todas as suas fases.

d) receber e conferir os serviços verificando a sua compatibilidade com as especificações estabelecidas, rejeitando, no todo ou em parte, se houver irregularidades.

e) efetuar os pagamentos à contratada de acordo com as condições de preço e prazo estabelecidas neste Instrumento.

f) comunicar formalmente à contratada quaisquer falhas verificadas no cumprimento da execução contratual, preferencialmente por meio eletrônico (e- mail).

7.4. Obrigações da contratada

7.4.1. Além do cumprimento de condições previstas Termo de Referência, deverá atender às seguintes obrigações gerais e especificas:

a) indicar preposto para representá-la na execução do objeto contratual, com capacidade para tomar decisões compatíveis com os compromissos assumidos, quando for o caso.

b) prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e, inclusive, às recomendações aceitas pela boa técnica.

c) responsabilizar-se pelo cumprimento da legislação de âmbito federal, estadual e municipal, pertinente ao objeto contratado.

d) executar o objeto da contratação rigorosamente de acordo com este instrumento e com as normas e especificações técnicas.

e) manter, durante a vigência contratual, todas as condições de habilitação exigidas para a contratação, comunicando ao contratante a superveniência de fato impeditivo da manutenção dessas condições.

f) responder pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução contratual.

7.5. É vedado à contratada:

7.5.1. Subcontratar ou sub-rogar (ceder ou transferir) total ou parcialmente a contratação.

7.5.2. Caucionar ou utilizar a Nota de Empenho para qualquer operação financeira.

8. DAS CONDIÇÕES DE PAGAMENTO:

8.1. Pagamento será realizado em até 07 (sete) dias úteis, após a apresentação do relatório mensal juntamente com emissão da Nota fiscal.

8.2. Não será admitida proposta com condição de pagamento diferente daquela definida no item anterior.

9. DOS RECURSOS ORÇAMENTÁRIOS:

9.1. Para efetivação desta contratação, há disponibilidade orçamentária, conforme previsto em:

3.3.90.40.00 Serviços de Tecnologia da Informação e Comunicação - TIC
3.3.90.40.99.00 Outros Serviços de Tecnologia da Informação
Ficha 010 e 039

10. DAS SANÇÕES:

10.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133/2021, quais sejam:

10.1.1. dar causa à inexecução parcial do contrato;

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

10.1.3. dar causa à inexecução total do contrato;

10.1.4. deixar de entregar a documentação exigida para o certame;

10.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

10.1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

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

10.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

10.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

10.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

10.1.12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

10.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

10.2.1. Advertência pela falta do subitem 10.1.1 deste regulamento de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

10.2.2. Multa será aplicada à contratada que der causa à inexecução parcial da(s) contratação(ões), nas seguintes proporções:

a) moratória de 10% (dez por cento) sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

b) moratória de 15% (quinze por cento) sobre o valor da parcela inadimplida, até o limite de 45 (quarenta e cinco) dias;

c) A partir do 46º (quadragésimo sexto) dia estará caracterizada a inexecução total da obrigação assumida, sujeitando-se, a contratada, à multa de 20% (vinte por cento) sobre o valor total estimado do contrato, autorizando a Administração a promover a extinção do ajuste por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei nº 14.133/2021.

10.2.3. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 10.1.2 a 10.1.7 deste regulamento de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

10.2.4. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 10.1.8 a 10.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

10.3. Na aplicação das sanções serão considerados:

10.3.1. a natureza e a gravidade da infração cometida;

10.3.2. as peculiaridades do caso concreto;

10.3.3. as circunstâncias agravantes ou atenuantes;

10.3.4. os danos que dela provierem para a Administração Pública;

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

10.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

10.5. A aplicação das sanções previstas neste regulamento de Contratação Direta, em hipótese alguma a obrigação de reparação integral do dano causado à Administração Pública.

10.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

10.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133/2021, e subsidiariamente na Lei nº 9.784, de 1999.

11. DOS ESCLARECIMENTOS E DAS INFORMAÇÕES:

11.1. A presente dispensa encontra-se disponível no sitio oficial da Fundação - https://fema.edu.br/index.php/compraselicitacoes, sendo que a mesma também poderá ser solicitada pelo e-mail: materiais@fema.edu.br

11.2. Os pedidos de esclarecimentos referentes à Dispensa deverão ser enviados ao responsável pela sua condução e operacionalização em até 1 (um) dia útil anterior à data estipulada referente ao limite de entrega das propostas, pelo e-mail materiais@fema.edu.br.

11.3. Os pedidos de esclarecimentos apresentados fora de prazo, não serão recebidos.

12. DAS DISPOSIÇÕES GERAIS:

12.1. O procedimento será divulgado no Portal Nacional de Contratações Públicas - PNCP e no sítio eletrônico www.fema.edu.br.

12.2. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste regulamento de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

12.3. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de qualquer ato emitido pela Administração.

12.4. No julgamento das propostas e da habilitação, a Administração poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

12.5. As normas disciplinadoras deste regulamento de Contratação Direta serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

12.6. Os fornecedores assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo de contratação.

12.7. Em caso de divergência entre disposições deste regulamento de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste regulamento.

13. ANEXOS

13.1. Integram este regulamento de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência;

ANEXO II – Modelo de proposta;

ANEXO III – Declarações diversas.

Assis, 17 de Abril de 2024.

Hilário Vetore Neto
Diretor Executivo

ANEXO I
TERMO DE REFERÊNCIA

1. OBJETO

1.1. A presente termo de referência tem como objeto a Contratação de empresa especializada na prestação de Serviços Gerenciados de Tecnologia da Informação como Serviços Gerenciados de Segurança da Informação devidamente descritos e caracterizados nas especificações técnicas presente abaixo:

LOTE - SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO		
ITEM	**DESCRIÇÃO**	**QTD**
1	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	5 meses
2	SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO	5 meses
3	SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE INFRAESTRUTURA	5 meses
4	SERVIÇO DE BACKUP EM NUVEM	5 meses

1.1.1. Os equipamentos utilizados pela contratada para prestação dos serviços deverão ser novos ou seminovos, ainda em linha de produção em pleno funcionamento, e cobertos por garantia pelo respectivo fabricante durante toda a vigência do contrato.

1.1.3. O prazo para ativação dos serviços do presente certame é de até 30 (trinta) dias corridos.

ITEM 1: Serviços Gerenciados de Segurança da Informação

Solução de Firewall de Próxima Geração

A contratada deverá fornecer uma solução de firewall de próxima geração (NGFW – Next Generation Firewall) em alta disponibilidade, no modo Ativo-Passivo, ou seja, no mínimo um equipamento disponível para assumir o funcionamento automaticamente, caso o principal fique indisponível;

Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos fornecidos como serviço e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam de responsabilidade do contratante;

Os equipamentos devem ser iguais e suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:

Especificações Gerais:

O equipamento proposto deve fornecer logs e relatórios embarcados contendo no mínimo os itens abaixo:

Dashboard com informações do sistema:

Informações de CPU
Informações do uso da rede.
Informações de memória.
Informações de atividades de navegação.
Permitir visualizar número políticas ativas.
Visualizar número de usuários conectados remotamente.
Visualizar número de usuários conectados localmente.
Relatórios com informações sobre as conexões de origem e destino por países.
Relatórios informando as conexões dos hosts.
Visualizar relatórios por período de tempo, permitindo o agendamento e o envio destes relatórios por e-mail.
Permitir exportar relatórios para as seguintes extensões/plataformas:
PDF
HTML
Excel
Permitir visualizar relatório de políticas ativas associado ao ID da política criada.
Relatório que informe o uso IPSEC por host e usuário.
Relatório que informe o uso L2TP por host e usuário.
Relatório que informe o uso PPTP por usuários.
Relatório abordando eventos de VPN.
Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:
Logs do sistema;
Logs das políticas de segurança;
Logs de autenticação;
Logs de administração do firewall NGFW.
Permitir ocultar dos relatórios usuários e IPs cadastrados.
Possuir no mínimo 8 interfaces 10/100/1000 base-T e 2 SFP 1GbE;
Possuir no mínimo 2 interfaces SFP+ 10GbE base-SR, com seus devidos transceivers e cabo de no mínimo 1 metro;
Deve suportar adição futura de no mínimo 2 interfaces 40GbE QSFP+;
Deve possuir no mínimo 2 portas que suportem by-pass;
A contratada deverá fornecer todos os cabos e seus acessórios necessários para atender os itens deste documento.
A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte:

Suportar no mínimo 6 (seis) Gbps de rendimento (throughput) de NGFW (next-generation firewall);
Suportar no mínimo 200.000 (duzentas mil) novas conexões por segundo;
Suportar no mínimo 17.500.000 (dezessete milhões e quinhentas mil) conexões simultâneas;
Possuir no mínimo 33 (trinta e três) Gbps de rendimento (throughput) do Firewall para pacotes UDP;
No mínimo 8.5 (oito inteiros e cinco décimos) Gbps de rendimento (throughput) do IPS;
Possuir no mínimo 3.2 (três inteiros e dois décimos) Gbps de throughput de VPN AES.
A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
A solução proposta deve possuir no mínimo 180 GB de espaço em disco SSD para o armazenamento local de eventos e relatórios.
Possuir slot para adição de módulo de portas;
Possuir ao menos uma porta console RJ45 ou similar;
Número irrestrito de usuários/IP conectados.
O equipamento deve ter no máximo 2 (dois) U de altura para montagem em rack 19".

Especificações da Administração, Autenticação e Configurações em geral

A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.
A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário.
O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.
A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.
A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.
A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.
Suporte à autenticação do Chromebook.

Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.
Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.
Certificados de autenticação para iOS e Android.
A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
A solução proposta deve suportar NTP.
A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
A solução proposta deve ter suporte multilíngue para console de administração web.
A solução proposta deverá suportar fazer um rollback de versão.
A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.
A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.
A solução proposta deve suportar SNMP v1, v2c.
A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.
A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação).
A solução proposta deve ter suporte a ambientes de terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
A solução proposta deve suportar:
Serviço de DHCP/DHCPv6;
Serviço de DHCP/DHCPv6 Relay Agent;
A solução proposta deve trabalhar como DNS/DNSv6 Proxy.

Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.
Permitir exportar informações de troubleshooting para arquivo PCAP.
Permitir o factory reset e troca do idioma via interface gráfica.
Reutilização de definições de objetos de rede, hosts, serviços, período de tempo, usuários, grupos, clientes e servers.
Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades especificas a ele.
Controle de acesso e dispositivos por zoneamento.
Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.
Traps SNMP ou e-mail para notificações do sistema.
Suportar envio de informações via Netflow e possuir informações via SNMP;
Ter funcionalidade que permita que o administrador manualmente atribua núcleos ("cores") do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.
Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet

A solução proposta deve suportar o balanceamento de carga e redundância para no mínimo 2 (dois) links de Internet.
A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.
A solução proposta deve suportar algoritmo "Round Robin" para balanceamento de carga.
A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.
A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.
A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).
A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

Especificações de Alta Disponibilidade

A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e

ativo/passivo.

A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.

O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.

A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".

A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

Especificações do Firewall e roteamento

A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.

A solução proposta deve suportar "Stateful Inspection" baseado no usuário "one-to-one", NAT Dinâmico e PAT.

A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.

A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso.

A solução proposta deve suportar arquitetura de segurança baseado em Zonas.

A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".

A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.

A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).

A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.

A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.

O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.

O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.
A solução proposta deve suportar IPv6.
A solução proposta deve suportar implementações de IPv6 Dual Stack.
A solução proposta deve suportar tuneis 6in4, 6to4, 4in6,6rd.
A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.
A solução proposta deve suportar DNSv6.
A solução proposta deve oferecer proteção DoS contra ataques IPv6.
A solução proposta deve oferecer prevenção contra Spoof em IPv6.
A solução proposta deve suportar 802.3ad para Link Aggregation.
A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.
A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.
Flood protection, DoS, DDoS e Portscan.
Bloqueio de Países baseados em GeoIP.
Suporte a Upstream proxy.
Suporte a VLAN DHCP e tagging.
Suporte a Multiple bridge.
Funcionalidades do portal do usuário.
Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).
Download dos clientes de autenticação disponibilizados pela ferramenta.
Download do cliente VPN SSL em plataformas Windows.
Download das configurações SSL em outras plataformas.
Informações de hotspot.
Autonomia de troca de senha do usuário.
Visualização do uso de internet do usuário conectado.
Acesso a mensagens em quarentena.
Opções base de VPN.
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.
L2TP e PPTP.
VPN SSL, IPSEC.

Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

Funcionalidades base de QoS e Quotas

QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.

Otimização em tempo real do protocolo Voip.

Suporte a marcação DSCP.

Regras associadas por usuário.

Criar regras que limitem e garantam upload e download.

Permitir criar regra de QoS individualmente e compartilhada.

Filtragem e Segurança Web

Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.

Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92 categorias oferecidas pela solução.

Realizar autenticação dos usuários nos modos transparente e padrão.

As autenticações devem ser feitas via NTLM.

Possuir sistema de quotas aplicado por usuários e grupos.

Permitir criar políticas por horário aplicado a usuários e grupos.

Possuir sistema de malware scanning que realize as seguintes ações:

Bloquear toda forma de vírus

Bloquear malwares web

Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

Prover proteção em tempo real de todos os acessos web.

A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.

Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.

Fornecer Pharming Protection.

Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.

Permitir criação de regras customizadas baseadas em usuário e hosts.

Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.
Validação de certificado.
Prover cache de navegação, contribuindo na agilidade dos acessos à internet.
Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.
Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.
Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
Range aceitável de 1 a 25600KB.
Bloquear trafego que não segue os padrões do protocolo HTTP.
Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
Nas exceções, permitir definir operadores "AND" e "OR".
Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.
Permitir criar regras de exceções por endereços IPs de origem.
Permitir criar regras de exceções por endereços IPs de destino.
Permitir criar exceções por grupo de usuários.
Permitir criar exceções por categorias de sites.
Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.
Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: "Criminal Activities, Finance & Investing, Games and Gambling", entre outras.
Permitir editar grupos de categorias pré-estabelecidos pela solução.
Deve ter sistema que permita a criação de novas categorias com as seguintes

especificações:
Nome da regra;
Permitir criar uma descrição para identificação da regra.
Ter a possibilidade de classificação de pelo menos: Produtivo ou Não produtivo;
Permitir aplicar Traffic shaping diretamente na categoria.
Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.
Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.
Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.
Ter função para criar grupos de URLs.
A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.
Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.
Deve permitir que em uma mesma política seja aplicada ações diferentes de acordo com o usuário autenticado.
Nas configurações das políticas, deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.
Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.
Permitir criar cotas de navegação com os seguintes requisitos:
Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

Controle e Segurança de Aplicações

Prover controle para mais de 2600 aplicações diferentes.
Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
Permitir criar regras de controle por usuário e hosts.
Permitir realizar traffic shaping por aplicação e grupo de aplicações.
Possibilitar que as regras criadas baseadas em aplicação permitam:
Bloquear o trafego para as aplicações

Liberar o trafego para as aplicações
Criar categorização das aplicações por risco:
Risco muito baixo
Risco baixo
Risco médio
Risco alto
Risco muito alto
Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.
Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.
Permitir agendar um horário e data específico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

Proteção de Redes

Prover funcionalidade de Intrusion Prevention System (IPS)
Proporcionar alta performance na inspeção dos pacotes
Possuir mais de 6500 assinaturas conhecidas.
Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.
Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.
Possuir funcionalidade Anti-DoS.
Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:
SYN Flood
UDP Flood
TCP Flood
ICMP Flood
IP Flood
Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ, e etc.

Possuir proteção contra spoofing.
Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.
Possuir funcionalidade para o administrador poder criar by-pass de DoS.
Permitir o administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.
Possuir proteção avançada contra ameaças persistentes (APT)
Detectar e bloquear tráfico de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.
Possuir logs e relatórios que informem todos eventos de APT.
Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.
Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.
Proteção para E-mails
Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.
Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.
Bloquear SPAN e MALWARES durante a transação SMTP.
Possuir duas engines de antivírus para duplo escaneamento.
Ter proteção em tempo real, a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança caso necessário.
Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.
Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.
Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customiza-los de acordo com o desejado.
Ter suporte a criptografia TLS para SMTP, POP e IMAP.
As ações dos e-mails considerados SPAN devem ser:
Drop
Warn
Quarantine

Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: [SPAN] Marketing etc. etc. etc.
Permitir visualizar os e-mails que se encontram na fila para serem enviadas.
Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.
Possuir funcionalidade de allowlist e blocklist.
Possuir funcionalidade que rejeite e-mails com HELO invalido e/ou que não possuam RDNS.
Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.

Quarentena de E-mail

Possuir quarentena para os e-mails e opções de notificações para o administrador.
E-mails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.
O usuário deve poder gerenciar sua quarentena de e-mails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.
As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.
Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.
Possuir funcionalidade de criptografia de e-mails e DLP para os dados
Possuir funcionalidade de encriptação de e-mails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.
Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF.
Ter como funcionalidade a possibilidade de o usuário poder registrar sua própria senha de segurança para que seja possível abrir os e-mails criptografados.
Possuir também funcionalidade para geração de senhas aleatórias para descriptografar o conteúdo.
Permitir enviar anexos junto aos e-mails criptografados.
Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não se deve utilizar qualquer software adicional, plugin, ou client instalado no equipamento.

Possuir funcionalidade de DLP nos E-mails
A engine de DLP deve ser automática na hora de escanear os e-mails e anexos, assim identificando todos os dados sensíveis encontrados no e-mail sem qualquer intervenção.
Ter a opção de criar exceções individuais para cada tipo de situação.
As regras devem corresponder para as redes de origem e alvos específicos como a especificados por URLs.
Suporte a operadores lógicos
Poder definir tamanho máximo para escaneamento.
Permitir bloquear e liberar ranges IP.
Suporte para utilização de Wildcards
Anexar automaticamente um prefixo/sufixo para autenticação.

Proteção para proteção de servidores WEB (WAF)

Possuir funcionalidade de proxy reverso
Possuir engine de URL hardening e prevenção a directory traversal.
Possuir engine Form hardening.
Proteção contra SQL injection
Proteção contra Cross-site scripting
Possuir duas engines de antivírus disponíveis para análise de malware.
Permitir definir o fluxo que o antivírus irá atuar, se será no upload ou download.
Permitir limitar o tamanho máximo em que o antivírus irá atuar.
Permitir bloquear conteúdo considerado unscannable.
Possuir HTTPS (SSL) encryption offloading.
Proteção para cookie signing com assinaturas digitais.
Possuir Path-based routing.
Suporte ao protocolo do Outlook anywhere.
Possuir autenticação reversa para acesso aos servidores web.
Permitir criar templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.
Ter abstração de servidores virtuais e físicos.
Proporcionar função de load balance para que os visitantes possam ser jogados para diversos servidores de forma transparente.
Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.
Bloquear clients com má reputação.
Bloquear protocolos com anomalias.

Limitar número de requisições.

Proteção de Sandbox na nuvem

Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.

Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.

Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll.

Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.

Realizar analise em documentos PDF.

Realizar analise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet

Suporte a mais de 20 tipos de arquivos e extensões.

Realizar analises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.

Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.

O tempo em média das análises devem ser menores do que 120 segundos.

Suportar a análise de links de download em tempo real.

Permitir escolher pelo menos duas regiões para as quais os arquivos para analise devem ser enviados.

Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para analisa.

Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.

O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.

Solução de gerenciamento

A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela contratante.

A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplica-los todos de uma única vez.

As políticas de configurações devem ter no mínimo as seguintes opções:

Proteção e políticas de acesso web

Controle de aplicativos

IPS

VPN
E-mail
Firewall
A solução deverá oferecer funcionalidade que permita o administrador criar templates de configuração para que o administrador possa aproveitar as mesmas regras para novos firewalls NGFWs.
Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.
Possuir múltiplas formas de customização de warning thresholds.
Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferencia-los como por exemplo: Região, modelo ou outro parâmetro.
Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos com diferentes funções.
Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

Ferramenta de relatórios e gestão de logs

A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;
A CONTRATADA deve disponibilizar no mínimo 500GB líquido para armazenamento de logs;
A solução deve suportar no mínimo 250 eventos por segundo ou 10GB de logs por dia;
A ferramenta de relatórios deverá suportar no mínimo os seguintes relatórios:
Ataques detectados;
Categorias de aplicações mais acessadas;
Categorias WEB mais acessadas;
Aplicações WEB mais utilizadas
Websites mais acessados;
Usuário ou equipamento com maior consumo de banda;
Usuário ou equipamento com maior número de sessões;
Aplicações de Maior Risco;
Aplicações com maior vulnerabilidade;
Top Malware, Botnets, Spyware e Adware detectados;
Usuários ou dispositivos com maior risco;
Aplicações mais acessadas;

Redes sociais mais acessadas;
Aplicações de streaming de áudio e vídeo mais acessadas;
Aplicações P2P mais acessadas;
Aplicações de Game mais acessadas;
Permitir a personalização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.
Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails cadastrados.
Ter fácil identificação das atividades de rede e ataques em potencial.
Armazenar histórico dos relatórios em disco local.
Possuir relatórios únicos para cada um dos módulos ofertados pela solução.
Possuir múltiplos formatos de relatório, pelo menos tabular e gráfico.
Permitir exportar relatórios para: PDF, Excel e HTML.
Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia e Google.
Possuir relatórios que informem principais atividades em cada módulo.
Ter logs em tempo real.
Ter logs arquivados para consulta posterior.
Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.
Possuir logs de auditoria.
Ter sua gerência totalmente baseada em acesso web.
Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades especificas na ferramenta.
Possuir no mínimo 2 (duas) dashboard sendo uma exclusiva para os relatórios e outra exclusiva para visualização da saúde do equipamento (CPU e memória).
O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.
Ter total gerência sobre a retenção dos dados armazenados neste equipamento.
Ter disponibilidade em firewall NGFW virtual e software caso necessário instalar o firewall NGFW em um hardware baseado em Intel.

ITEM 2: Serviço de Proteção para Estações de Trabalho e Servidores

A solução deve ser licenciada para todo o parque de TIC da FEMA, ou seja, para 300 (trezentos) dispositivos, servidores ou estações de trabalho.
Será de responsabilidade da contratada administrar e suportar a solução de proteção, garantido o pleno funcionamento do serviço.

Console de Gerenciamento

O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor;

O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS);

O acesso ao Console deve suportar várias sessões simultâneas;

Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor;

Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases:

Microsoft Windows 10 e 11

Microsoft Windows Server 2012, 2012 R2, 2016 e 2019;

Ubuntu Server e Desktop 14.04, 16.04.1, 18.04.1 e 22.04;

CentOS 6 e 7;

Debian 11 e 12;

Fedora 29 e 39;

O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE;

Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo;

Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso);

Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

Descobrir automaticamente as estações da rede que não possuem o cliente

instalado através de funcionalidade integrada ao console de gerenciamento;
Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;
A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente;
Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador);
O log deve ser centralizado e conter, no mínimo, os seguintes itens:
Nome da ameaça
Nome do arquivo infectado
Data e hora da infecção
Ação tomada
Endereço IP da máquina
Usuário autenticado na máquina
Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado via rede;
O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques;
Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

Atualização de Vacinas

Atualização incremental e on-line das vacinas;
Atualização em clientes móveis (notebook, laptop, netbook, ultrabook, e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador;
Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet;
Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante;
Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função;
Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução;

Qualquer atualização deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la;
Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;
O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

Cliente Gerenciado

A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits;
O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:
Microsoft Windows 10 e 11
Microsoft Windows Server 2012, 2012 R2, 2016 e 2019;
Ubuntu Server e Desktop 14.04, 16.04.1, 18.04.1 e 22.04;
CentOS 6 e 7;
Debian 11 e 12;
Fedora 29 e 39;
O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede;
O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento;
Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante;
Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento;
Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária;
O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas (*locked*) através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

Funcionalidade de Firewall e Sistema de Prevenção de Intrusão (IPS)

A funcionalidade deve suportar os protocolos TCP e UDP;

Reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio;

Possuir proteção contra-ataques de *Denial of Service (DoS), Port-Scan* e *Spoofing e botnet*;

Possibilidades de criação de assinaturas personalizadas para detecção;

Possibilidade de agendar a ativação de novas regras do *firewall*;

Possibilidade de criar regras diferenciadas por aplicações;

todos os executáveis da lista ou liberar somente os executáveis da lista;

Bloqueio de ataques baseado na exploração da vulnerabilidade;

Permitir integração com navegadores WEB para prevenção de ataques;

Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.

Funcionalidade de Antimalware

A solução deve prover proteção em tempo real contra vírus, *trojans*, *worms*, spyware, *adwares* e outros tipos de códigos maliciosos;

As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução;

Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real);

Permitir verificação das ameaças de maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;

Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes;

Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar;

Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP;

Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados;

Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:

CAB;

ZIP;

RAR;

LHA;
ARJ;
TAR;
Capacidade de terminar o processo e serviço da ameaça no momento de detecção;
Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede;
Possibilidade de bloquear verificação de malware em recursos mapeados da rede;
Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos;
Não serão aceitas soluções de Antimalware que possuam engine de terceiros;
Permitir o bloqueio da execução de aplicações baseado em nome e pasta.

Funcionalidade de Reconhecimento de Novas Ameaças

A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;
Capacidade de detecção de *keyloggers* por comportamento dos processos em memória;
Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts;
Capacidade de detecção de *Trojans* e *Worms* por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção;
Possibilidade de agendar a varredura da detecção de novas ameaças.
Uso de sandboxing na nuvem para analisar o comportamento de malwares, com SLA de 5 minutos até 1 hora de resposta.

Funcionalidade de Controle de Dispositivos

Controlar o uso de dispositivos com comunicação infravermelha, *firewire*, portas seriais e paralelas, através de mecanismos de permissão e bloqueio, identificando-os pelo "Class ID" e pelo "Device ID";
Permitir criar políticas de bloqueio de dispositivos distintas para diferentes grupos da base de estações conectadas;
Gerenciamento integrado à console de gerência da solução.
A solução deve ser capaz de permitir ou negar o uso dos dispositivos com base nos seguintes critérios:
Fabricante
Modelo
Número de Série

Funcionalidade de Controle WEB

Controlar acesso a sites, possibilitando o bloqueio do mesmo;

Permitir criar políticas de bloqueio com base em categorias e lista de URL;

Permitir gerar relatórios de sites acessados e bloqueados;

Relatórios e Monitoramento

Gerar, no mínimo, os relatórios abaixo descritos, tanto de maneira gráfica quanto em arquivos CSV, PDF, HTML ou MHTML, permitindo escolher o período de consulta desejado:

Listagem dos malwares que infectaram determinada máquina;

Listagem das máquinas que estão infectadas por determinado *malware*;

Relatório dos totais de códigos maliciosos detectados, indicando aqueles de maior incidência;

Listagem das máquinas nas quais o antimalware deixou de remover algum código malicioso;

Número total de arquivos maliciosos removidos;

Relatório de máquinas cuja atualização de componentes do software antimalware e assinaturas não foi realizada, incluindo a data da última atualização;

Relatório de máquinas com maior número de infecções;

Relatório de atualização de componentes do software antimalware e assinaturas;

Relatório das máquinas que não se comunicaram com o servidor de antimalware a partir de uma determinada data.;

Possibilidade de exibir a lista de servidores e estações que possuam o antimalware instalado, contendo informações como nome da máquina, usuário autenticado, versão do *engine*, data da vacina, data da última verificação e status;

Sumário de eventos IPS por assinatura, por alvo, por endereço IP de origem, principais nós atacados, principais assinaturas;

Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.

Deverá ter um console de administração de licenças em nuvem, de onde é possível revisar os detalhes de equipamentos aos quais foram provisionados o licenciamento.

Funcionalidades Tecnológicas

A console deverá funcionar também através de um Appliance Virtual.

Dentro do módulo de firewall deverá possuir a funcionalidade de bloqueio de exploits.

Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

Deverá contar com um filtro de correio para a detecção de malware e spam.
Deverá ser uma solução que pode ser utilizada e administrada através de um console de administração remota de antivírus para os sistemas operacionais Windows, Linux e Mac.
A solução Anti Malware deverá contar com a tecnologia HIPS (Host-based Intrusion Prevention System) para proteger a manipulação indevida e detectar ameaças com base na conduta do host.
O produto deverá ter um controle web para limitar o acesso a sites web por categoria, além de poder mostrar ao usuário uma notificação de bloqueio.
Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.
O firewall do produto deverá ser bidirecional, assim como detectar as redes seguras.
A solução deverá realizar exploração em estado inativo para poder fornecer desta forma uma proteção pró ativa enquanto o equipamento não está em uso.
A console de administração deverá ter um Appliance Virtual aberto para instalar e utilizar em ambientes virtuais, para ter um ambiente distribuído e de fácil instalação.
O acesso ao console de administração do antivírus deve ser feito com duplo fator de autenticação integrado dentro da mesma console aonde é possível ativa-lo se a necessidade de nenhum add-on adicional.
O console de administração de licenças deve ser na nuvem, aonde é possível revisar os detalhes dos equipamentos que estão utilizando a licença do antivírus.
A console de administração deverá suportar a instalação em ambiente com sistema operacional Linux.
Detecção do malware por DNA do vírus.
Deverá ter a capacidade de atualizar os patches do sistema operacional.
A solução deve ser capaz de definir uma lista de usuários específicos que podem fazer utilização dos dispositivos. Para dispositivos de armazenamento a solução deve permitir a configuração das seguintes permissões: Leitura e Escrita, Bloqueio, Somente Leitura e Advertência.
Quando se conectar ou utilizar um dispositivo de armazenamento a solução de antivírus deve proporcionar as seguintes opções: Escancear, Não realizar nenhuma ação e Se lembrar dessas ações.
Deverá permitir a execução remota de scripts, arquivos batches e pacotes personalizados através da console.
Deve permitir gerar grupos de clientes dinâmicos e grupos estáticos.
O fabricante deverá proporcionar ao menos três formas diferentes de realizar a

instalação do console de administração remota: Instalação Tudo em Um, Instalação por Componentes e em Appliance Virtual.

O Appliance Virtual deverá suportar ao menos as seguintes plataformas de virtualização: VMWare vSphere, Oracle Virtual Box, Microsoft Hyper-V e Azure.

A console de administração deverá suportar a instalação em Linux.

Deve contar com desinstalador de antivírus de terceiros.

A solução de proteção Antispam deve realizar as verificações utilizando o protocolo SSL.

A solução antivírus deve contar um Firewall pessoal com os seguintes modos de configuração: Modo automático, Modo Interativo, Modo baseado em políticas e Modo de Aprendizagem.

O fabricante deverá ter suporte local em idioma português.

O fabricante deverá ter documentação publicada na internet no idioma português.

Possuir proteção contra ransomware, com um módulo específico, utilizando a console para configuração e distribuição de políticas aos endpoints.

Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push (EPNS).

Funcionalidade de Inventário de Hardware (CPU, RAM, Armazenamento, Versão de Sistema Operacional e Periféricos conectados)

Possuir no mínimo 31 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.

Quarentena do Correio Eletrônico

Mensagens de e-mail de spam e de quarentena podem ser armazenadas em um sistema de arquivos local, não no banco de dados de caixa de correio do Exchange.

A criptografia e a compactação de arquivos de e-mail em quarentena devem ser armazenadas localmente.

Arquivos de email em quarentena excluídos podem ser restaurados usando a interface de linha de comando do produto do fabricante do produto de proteção de email (desde que eles ainda não tenham sido excluídos do sistema de arquivos).

Os relatórios de quarentena devem ser enviados para um endereço de email especificado usando uma tarefa agendada.

É possível armazenar mensagens de destinatários inexistentes: aplica-se a mensagens marcadas para serem colocadas em quarentena por proteção antivírus, proteção antispam ou regras.

O administrador da Quarentena de e-mail deve estar disponível nos três tipos de quarentena: Quarentena local, Correio electrônico de quarentena e Quarentena de

MS Exchange
Deve ter uma interface da Web da Quarentena da Web.
Deve ter validação de mensagem com SPF, DKIM e DMARC, localmente no mesmo servidor de email no aplicativo de proteção de email.
Para verificar o banco de dados por demanda, deve usar a API do EWS (Serviços Web do Exchange) para se conectar ao Microsoft Exchange Server usando HTTP / HTTPS.
A proteção de email deve ter a possibilidade de instalar por componentes, você pode escolher os componentes para adicionar ou remover.
O produto de segurança deve ter uma interface de linha de comando que ofereça aos usuários e administradores avançados opções mais profundas para gerenciar o produto.
As regras de correio devem ser classificadas em três níveis e avaliadas na seguinte ordem:
Regras de filtragem: regra avaliada antes do antispam e da verificação antivírus
Regras de processamento de anexos: regra avaliada durante a verificação antivírus
Regras de processamento de anexos: regra avaliada durante a verificação antivírus
Deve poder explorar mensagens de conexões autenticadas ou internas.
A solução deve ser capaz de excluir o cabeçalho SCL existente antes da verificação e pode ser desativada se for necessário manter o cabeçalho do nível de confiança em relação ao spam.

Regras

Deve-se poder excluir o anexo de uma mensagem no Transporte de Email, no banco de dados da caixa de correio e na verificação do banco de dados.
Deve-se poder adicionar uma string personalizada ao campo de cabeçalho (ao cabeçalho da mensagem).
Deve ser possível adicionar várias ações para uma regra.

Condições

Deve-se poder aplicar a mensagens enviadas a um destinatário validado no Active Directory sobre proteção de transporte de email.
Deve-se poder aplicar condições a mensagens que tenham anexos com nomes específicos.
Deve-se poder aplicar condições a mensagens de um remetente com um domínio específico no endereço de e-mail.
Deve ser possível analisar se a mensagem contém um arquivo danificado na proteção de transporte de email e na proteção de banco de dados da caixa de

entrada de email.

O produto deve suportar múltiplas funções Microsoft Exchange Server 2007, 2010 e Windows SM 2008 e 2011, proteção contra spam, regras, sobre proteção de transporte de e-mail, varredura de banco de dados sob demanda, proteção de banco de dados dos dados da caixa de correio e da quarentena.

O produto deve suportar borda e caixa de correio, Windows Exchange Server 2016, proteção contra spam, regras, proteção de transporte de email, verificação de banco de dados sob demanda e quarentena de email.

ITEM 03: Serviço de Suporte Técnico e Monitoramento de Infraestrutura

Para garantir a continuidade e qualidade dos serviços ofertados neste lote e do ambiente atual de infraestrutura da contratante, devem ser monitorados e suportado pela contratada.

Sobre Chamados e Atendimento Técnico

A contratante poderá abrir chamados de manutenção através de chamada telefônica para número fixo, central de atendimento via navegador (WEB) ou correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da contratada;

O atendimento técnico presencial deverá ocorrer de segunda a sexta-feira (exceto feriados) das 09:00h às 18:00h, sob demanda;

O atendimento técnico remoto deverá ocorrer de segunda a sexta-feira (exceto feriados) das 08:00h às 18:00h;

Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software;

A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;

A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (fotocopias, etc), mídias de armazenamento de dados e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

A contratada deverá realizar atendimentos remotos à equipe de tecnologia da informação da contratante, a partir de solicitações recebidas dos técnicos ou gestores de contrato da contratante via sistema de atendimento, telefone ou correio eletrônico;

Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

Executar ações correlatas, que demandem maior esforço ou complexidade (ex: instalações e ou atualizações de software em grande quantidade de equipamentos, elaboração de roteiro específico, etc.), solicitadas diretamente pelo Gestor do Contrato por parte da Contratante e devidamente registradas no Sistema de atendimento técnico;

Deverá realizar configurações solicitadas pela contratante, tais como: regras de trafego de dados, rotas, políticas e demais configurações especificas dos componentes da solução;

Planejamento e aplicação de atualizações e ou correções de firmware com programação prévia de forma que não seja gerado nenhum tipo de indisponibilidade ou a mínima possível acordada com a contratante;

Realização de otimizações nas configurações para melhora do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela Contratante;

Na impossibilidade de resolução de problema técnico telefônico ou acesso remoto a contratada deverá disponibilizar uma visita presencial para avaliação e resolução do problema;

Deverá atualizar os softwares da solução sempre que disponíveis e homologados pelo fabricante. Acordando e alinhando as operações com a contratante;

A contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

Todo acesso remoto à rede da contratante, deve ser feito via VPN cliente-to-site;

O meto de autenticação remota na rede dever possuir duplo fator de autenticação, através de aplicativo mobile (iOS, Android), autenticação via Push, hard tokens, scripts em PowerShell e SMS;

Garantia de Tempo de Resposta e Nível de Serviço

A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Inicio do atendimento em até:
1	Serviço indisponível	30 minutos
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas

4	Manutenção preventiva	Programada

O acordo de nível de serviço para suporte técnico deverá obedecer ao seguinte escopo:

Prioridade	**Descrição**
1 (Emergencial)	O serviço está for a de operação ou há um impacto crítico nas operações dos negócios.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

As horas para primeiro atendimento e resolução de incidentes são horas úteis e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

Central de Chamados e Informações

A contratada deverá disponibilizar e gerenciar os atendimentos técnicas da contratante através de portal de gerenciamento de atendimentos com acesso através de navegador web;

Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;

A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

A contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;

A contratante deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;

O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da contratada, sendo essa responsável por sua atualização e manutenção;

A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;

O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;

A solução de atendimento e informações deverá constar com a possibilidade de cadastro e organização de ativos de rede, tais como: Firewall, Switches, dispositivos de rede e demais itens com acesso à rede;
A contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela contratante;
Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;
Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a contratante;
O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a contratante;
Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;
A solução deverá conter módulo que possibilite o inventário de racks dentro do data center;
Os itens de inventario da solução deverão permitir ser anexados aos atendimentos técnicos, criando assim uma relação de atendimento versus dispositivo da contratante;
A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";
A contratada deverá garantir que a solução de atendimento e informações tenha a possibilidade de cadastrar e organizar certificados digitais da contratante;
A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
Deverá ser possível a criação de grupos de usuários na solução;
A solução disponibilizada pela contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.

Monitoramento do Ambiente

A contratada deverá monitorar no mínimo 150 sensores ou itens, do ambiente de data center, infraestrutura de rede e equipamentos adquiridos neste documento;
A contratada deverá prover a solução de monitoramento como serviço, pelo prazo de 5 (cinco) meses;
A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;
Deverá ter SLA de disponibilidade da console de gerenciamento de no mínimo

99,98%;
A solução de monitoramento deverá estar hospedada em datacenter com a classificação mínima de Tier III ;
A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a contratante;
Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico;
Ser capaz de executar áudio pré-definido em caso de alteração de sensores de monitoramento;
Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;
Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;
O monitoramento deverá ser compatível com os principais serviços de nuvem pública;
O sistema de monitoramento deverá contar com aplicativo de administração instalável para o sistema operacional Microsoft Windows;
A solução deverá ser compatível com os seguintes protocolos:
SNMPv1;
SNMPv2;
SNMPv3;
WMI;
SSH;
Deverá ter intervalo mínimo de verificação de 30 (trinta) segundos para os sensores monitorados;
A solução deverá alertar sobre medições incomuns de sensores do ambiente, ou seja, deverá analisar padrões alertando quando houver um estado incomum no monitoramento;
Fornecer informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os paramentos estão ou não dentro dos limites preestabelecidos;
Deve permitir o monitoramento da performance com detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com carga de CPU, uso da memória, utilização de banda, status operacional de interface de rede, tempo de resposta dos dispositivos e eventos de erros;

Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos;
Permitir a configuração ou agendamento de descobrimento automático na rede;
Permitir a criação de relatórios de rede personalizados que possam ser exportados para pdf., impresso ou visualizado via HTTP;
Deve suportar IPV4 e IPV6;
Deve permitir interação na configuração do dispositivo através de SNMP v1, v2 e v3;
A solução de monitoramento deverá armazenar dados históricos armazenados em seu banco de dados interno pelo período de 90 (noventa dias);
A solução deverá permitir a personalização de disparadores para sensores, tais como: intervalo de tempo de monitoramento, intervalo de tempo entre erros e alertas e quantidade de alertas consecutivos;
Deverá ser capaz de efetuar detecções automáticas no ambiente da contratante;
A solução de monitoramento deverá ser capaz de entregar e-mails utilizando Relay autenticado;
Deverá ser possível o monitoramento de todas as portas das soluções (hardware) deste termo de referência, mostrando através de tabela de dados e gráficos sua disponibilidade e largura de banda com o intervalo mínimo de 30 (trinta) segundos;
A solução deverá monitorar características físicas das soluções (hardware) desta solução, tais como: temperatura do hardware, utilização de memória volátil, utilização de armazenamento, utilização e processamento e carga total do equipamento;
Deverá ter sensor com a informação de quantidade de tempo ligado dos equipamentos (hardwares) das soluções;
A solução de monitoramento deverá abrir chamado de maneira automática junto a contratante, após a alteração de um sensor para o estado de alerta ou erro;
Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;
Deverá ser possível a criação de templates de relatórios de monitoramento;
A solução deverá conter sensor de "*Sniffing de Pacotes*" para monitoramento de tráfego incluindo: tráfego por porta e endereço IP, tráfego total, tráfego web (http/https), tráfego de e-mail (IMAP/POP/SMTP), tráfego de transferência de arquivos (FTP e P2P), tráfego de infraestrutura (DHCP, DNS, ICMP e SNMP) e tráfego de acesso remoto (RDP, SSH e VNC);
Deverá suportar monitoramento de tráfego sFlow e Netflow;
Deverá suportar monitoramento nativo de firewall incluindo: status, tráfego inbond e

outbound para LAN e WLAN, eventos, atualizações, protocolos mais utilizados (Netflow) e conexões mais utilizadas (Netflow);

Deverá suportar o monitoramento da LAN, WAN e VPNs através de de SNMP, sFLOW, Netflow, Ping e Packet Sniffing;

Deverá suportar o monitoramento da rede WLAN incluindo: Tráfego, intensidade do sinal, status dos dispositivos e último acesso;

Deverá suportar o monitoramento dos seguintes Sistemas Operacionais: Microsoft Windows, Linux e MAC OS X

Deverá suportar o monitoramento das seguintes aplicações: Microsoft Active Directory, SQL Server, Hyper-V e VMWare

Deverá ser capaz de detectar automaticamente sobrecargas de largura de banda em equipamentos de rede gerenciáveis;

A solução deverá ser capaz de monitorar a qualidade de serviço da rede incluindo: jitter, QoS, latência, perda de pacotes, e MOS (mean opinion score);

Deverá ser capaz de monitorar a latência de um dispositivo;

A solução deverá ser capaz de importar arquivos ".MIB", interpreta-los e integra-los ao sistema de monitoramento;

Relatórios

Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com:

Relatório de Chamados (referente ao serviço descrito nesse lote):

Categoria do chamado;

Usuário;

Ativos relacionados;

Data de abertura e fechamento;

Status;

Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):

Disponibilidade;

Consumo de hardware (CPU, memória, disco, consumo de banda);

Alertas e erros;

Relatório de Segurança da Informação mensal:

Ataques detectados;

Categorias de aplicações mais acessadas;

Categorias WEB mais acessadas;

Categorias WEB mais bloqueados;

Aplicações WEB mais utilizadas;

Aplicações WEB mais bloqueadas;
Websites mais acessados;
Usuário ou equipamento com maior consumo de banda;
Aplicações de Maior Risco;
Usuários ou dispositivos com maior risco;
Consumo de banda da rede interna;
Relatório de vulnerabilidade trimestral:
Detectar vulnerabilidades em aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
Verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hot fixes, service packs, registros, peer to peer, portas de serviço habilitadas e antivírus;
Detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
Efetua descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional da universidade;
Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;
Scanner (varredura) de rede para identificar portas TCP/UDP abertas.
Riscos baseados na pontuação CVE (Common Vulnerabilities and Exposures);
Gerar relatório nos formatos XML, PDF, CSVe HTML;
Visualização de problemas por categoria;
Cinco níveis de severidade: Critical, High, Medium, Low, Info;
Os relatórios devem serem entregues mensalmente ao gestor do contrato, na data combinada, de forma eletrônica ou em reunião presencial.

Serviços de Instalação e Configuração

Esse item refere a toda instalação e configuração necessárias para efetuar a prestação de todos os serviços descritos nesse termo de referência.
A contratada deverá instalar e configurar os equipamentos alocados de forma físicas e lógicas seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;
Manter durante o período de serviço de instalação e configuração todas as condições de habilitação e qualificação exigidas;
Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa

técnica;

Prestar todos os esclarecimentos que lhe forem solicitados pelo contratante, atendendo prontamente a quaisquer reclamações;

Fornecer toda a mão-de-obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos fornecidos como serviço e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam de responsabilidade do contratante;

Instalação física de todos os equipamentos em Rack disponibilizado pela Contratante;

Os equipamentos devem estar com firmware e/ou software na versão mais recente e estável recomentada pelo fabricante da solução;

Características especificas do item 1:

Os equipamentos devem ser configurados em alta disponibilidade, no modo Ativo-Passivo, um equipamento disponível (configurado), para em caso de falha do equipamento Ativo, o Passivo assuma da operação automaticamente, sem a necessidade de intervenção;

A contratada deverá migrar ou executar configurações similares as configurações atuais implementadas no ambiente atual da contratante;

Em caso necessite de parada no ambiente, para efetuar a instalação do serviço, deverá ser acordado com a contratante antecipadamente;

Características especificas do item 4:

A contratada deve disponibilizar os recursos através de máquinas virtuais, com a quantidade de recurso e sistema operacional solicitado pela contratante.

A contrata deverá elaborar um plano de implementação junto a contratante, com: descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado "Projeto Executivo" tendo a visibilidade completa do projeto e seus status evolutivo. O documento deve ser entregue para contratante, analisado e aceito pelo responsável técnico da contratante;

A contratada deverá apresentar em reunião a conclusão do projeto com a entrega do documento "Projeto Executivo" completo, contendo todas as informações da operação, arquivos de backup das configurações e visão estratégia;

É responsabilidade da contratada falhas ou erros de instalação provenientes das

operações de instalação e configuração;
Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;
As senhas configuradas pela contratada no ambiente durante a instalação deverão ter requisito mínimo de 08 (outo) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;
Os profissionais técnicos alocados na operação pela contratada deverá estar devidamente identificado com uniforme bem como crachá de identificação;
A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente;

ITEM 04: Serviços Gerenciados de Backup

Ferramenta de backup em nuvem e Data Center

Será de responsabilidade da contratada implementar e configurar o software de transferência de backup local para o repositório na nuvem, de acordo com as políticas atuais da FEMA.
A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;
A contratada deverá ofertar o armazenar o backup da contratante em nuvem, com backups diários, com no mínimo as seguintes características:
Deverá conter um espaço mínimo liquido de 2TB de armazenamento em nuvem;
A solução deverá conter compactação e/ou aceleração WAN, para menor carga de utilização dos links de internet da contratante;
O licenciamento e operação do ambiente em nuvem é de total responsabilidade da contratada;
O armazenamento de dados da contratante deverá estar localizado no estado de São Paulo, mantendo assim uma menor latência na comunicação e transferência de dados;
A contratada deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados de backup da contratante. Se responsabilizando por qualquer dano causado a eles;
Os backups deverão estar criptografados com um mínimo de 256 bits;
Estar localizado no Brasil, ponto de maior concentração da estrutura do CONTRATANTE; estrutura física dedicada ao serviço de hospedagem, de modo a garantir um ambiente seguro e controlado e possuir ambientes definidos para computadores, sistemas de armazenamento, rede, administração predial, NOC, SOC e sala para clientes;

O data center deverá possuir a certificação Tier III ou ISO27001 ou SOC 2 Type 2;

Instalações Físicas

Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;

Possuir rack do tipo gabinete de 19";

Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento;

Energia Elétrica

Alimentação elétrica redundante;

Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;

Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local;

Climatização

Sistema de climatização redundante (n+1), refrigerado por formas diferentes;

Proteção Contra Incêndio

Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);

Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;

Segurança Física

Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;

Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;

Câmeras de circuito interno de televisão, monitoradas e gerenciadas, cujas imagens possam ser posteriormente consultadas e viabilizem o rastreamento de pessoas dentro do IDC;

Acesso ao local através de leitura biométrica;

O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;

Estrutura de Telecomunicações

Utilizar protocolo de roteamento inteligente para garantir um gerenciamento dinâmico

e otimizado dos múltiplos links, assegurar um melhor desempenho no acesso e maior redundância com relação à disponibilidade do acesso;
Possuir conexões redundantes responsáveis pelo tráfego interno, facilitando monitoramento e administração em diferentes pontos do data center;
Preferencialmente, possuir Pontos de Troca de Tráfego e Acordos de Peering que possam otimizar custos e benefícios com possíveis parceiros do CONTRATANTE;
Deverá ser construída uma rede local logicamente isolada para a CONTRATANTE dentro do Datacenter. Esta construção deverá ser feita através de VLANs configuradas sobre switches redundantes, permitindo a construção de múltiplos segmentos lógicos de rede para acomodar as tecnologias necessárias para aplicativos, backup de dados, monitoramento, gestão remota de aplicações, dentre outras.

Gestão de backup nuvem

A contratada deverá administrar e monitorar o sistema de backup descrito nesse documento;
Será de responsabilidade da contratada manter o pleno funcionamento da política de cópia de backup, de acordo com a rotina de backup estabelecida pela contratante;
Deverá monitorar diariamente, os relatórios de cópia de backup gerados ao concluir a tarefa, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da contratada efetuar correção ou ajuste técnico para a normalização do mesmo, garantindo o pleno funcionamento da solução;
A contratada deverá fornecer mensalmente, toda primeira segunda-feira do mês deverá ser entregue a contratante, um relatório com o resumo de execução de cada tarefa de cópia de backup, durante ao mês anterior, documento denominado "Relatório de Backup Nuvem Diário – MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;
Deverá ser de responsabilidade da contratada garantir integridade da cópia do backup LOCAL para NUVEM;
A contratada deverá fornecer mensalmente, um relatório com o resumo da execução dos testes automáticos de integridade das cópias de backups, referente ao mês anterior, documento denominado "Relatório de Teste de Cópia de Backup - MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;
A contratada deverá ser responsável por executar as restaurações conforme a manda da contratante;
Para controle, deverá ser entregue a contratante, um relatório de todas restaurações executadas, com data, motivo, objeto e solicitante, referente ao mês anterior,

documento denominado "Relatório de Restauração de Backup em Nuvem - MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;
Deverá ser realizada de maneira mensal uma reunião presencial com o gestor do contrato, onde a contratada deverá apresentar o relatório mensal.

2. DA NECESSIDADE DA CONTRATAÇÃO

Diante do crescente volume de dados operacionalizados em sistema, da amplitude e diversidade do parque tecnológico da FEMA e da grande dependência do negócio a disponibilidade e qualidade dos serviços de TIC, faz-se importante e necessário para proteger as atividades da FEMA contra eventuais ameaças cibernéticas mediante monitoramento de ambiente tecnológico, além de resposta imediata a segurança da informação.
A contratação se alinha aos objetivos citados na medida em que requerem cada vez mais ferramentas e soluções que proporcionem segurança, alta disponibilidade, eficiência, escalabilidade e ganho de desempenho na operacionalização de dados em sistemas com segurança contra eventuais ataques cibernéticos.

3. CONDIÇÕES DE PAGAMENTO:

3.1. Pagamento será realizado em até 07 (sete) dias úteis, após a apresentação do relatório mensal juntamente com emissão da Nota fiscal.

4. DESCRIÇÃO DA SOLUÇÃO

4.1. A demanda visa a prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças acessíveis na internet de superfície, profunda e oculta e resposta à incidentes de segurança da informação através da implantação de gerenciadores de segurança de informações.
4.2. Trata-se, portanto, de uma mescla de recursos de hardware, software e telecomunicações potencializados pela internet para melhorar os fluxos de comunicação nas instituições, refletindo também na qualidade dos serviços prestados.
4.3. Os resultados esperados com a solução serão:
a) Promover segurança contínua ao parque tecnológico da FEMA: Mitigar de forma continua, preventiva e reativa, possíveis ameaças ao ambiente computacional da FEMA que possam promover perda de dados.
b) Promover monitoramento contínuo ao parque tecnológico da FEMA: Monitorar todos os ativos de TIC, visando aplicar as polícias de segurança em um ambiente

tecnológico.
c) Controlar individualmente os ativos de TIC: Controlar individualmente os ativos da FEMA no que tange as vulnerabilidades detectadas e a disponibilidade, promover uma política de segurança ativa.
d) Promover robustez: Promover resiliência e disponibilidade ao ambiente suportado quando por ventura sofra com algum tipo de ataque, mantendo-se funcional e com qualidade.
e) Promover economia dos recursos públicos: Compor a prestação de serviços com requisitos técnicos mínimos que possam promover a concorrência pública, visando à economia nos recursos financeiros investidos, garantindo que os recursos disponibilizados sejam utilizados com eficiência e eficácia.

5. PRAZO DE VIGÊNCIA

5.1. O prazo de vigência do contrato será de 05 (cinco) meses.

6. DA EXECUÇÃO

6.1. Os serviços contratados deverão funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana durante todo o período da vigência do contrato.

7. LOCAL DE PRESTAÇÃO DOS SERVIÇOS

7.1. Os serviços serão prestados no Campus da FEMA – FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS E ANEXOS.

8. HORÁRIO, DURAÇÃO, PERIODICIDADE DA EXECUÇÃO DOS SERVIÇOS

8.1. Remissão ao item 7.1. Prazo de Execução.

9. FUNDAMENTO LEGAL

9.1. A contratação do objeto em pauta se sujeitará integralmente à Lei nº 14.133/2021.

10. CONTROLE E FISCALIZAÇÃO

10.1. O acompanhamento e a fiscalização da execução da contratação serão de responsabilidade da FEMA, e consistem na verificação da conformidade da execução.

11. DISPOSIÇÃO FINAL

11.1. Este termo de referência foi elaborado através das especificações técnicas contidas no Documento de Formalização de Demanda e Estudo Técnico Preliminares apresentados pela Coordenação do Centro de Pesquisa em Informática da FEMA, informações ou esclarecimentos deverão ser solicitados ao Setor de Compras, através dos e-mail materiais@fema.edu.br, os quais serão remetidos a respectiva coordenação.

ANEXO II

MODELO SUGERIDO DE PROPOSTA COMERCIAL

(Em papel timbrado da licitante)

PROCESSO Nº 008/2024

DISPENSA ELETRÔNICA Nº 002/2024 – SEM DISPUTA

1 – IDENTIFICAÇÃO DA EMPRESA

RAZÃO SOCIAL:		
CNPJ/MF:	INSCRIÇÃO ESTADUAL OU MUNICIPAL:	
ENDEREÇO:		N.°:
BAIRRO:	CIDADE:	
CEP:	ESTADO:	
FONE:	ENDEREÇO ELETRÔNICO:	

2 - OBJETO

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

3 - PREÇOS

Os preços ofertados para o objeto desta licitação, são os seguintes:

	ITEM	DESCRIÇÃO	QTDE	V.U	V.T
LOTE ÚNICO	**1**	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	5 meses		
	2	SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO	5 meses		
	3	SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE INFRAESTRUTURA	5 meses		
	4	SERVIÇO DE BACKUP EM NUVEM	5 meses		
VALOR GLOBAL:					

VALOR GLOBAL DA PROPOSTA: R$ 0,00 (valor por extenso) Obs.: Será considerado como PREÇO GLOBAL o preço referente a 05 (cinco) meses.

Declaramos total concordância com as condições da presente Contratação Direta.

Declaramos, também, que os valores acima ofertados estão incluídos, além dos lucros, todas e quaisquer despesas de responsabilidade do proponente que, direta ou indiretamente, decorram da execução do objeto da contratação.

Declaramos ainda, que os serviços prestados serão realizados de acordo com as condições e especificações desta contratação.

VALIDADE DA PROPOSTA: A validade da Proposta é de: _____ dias (mínimo de 30 dias).

Dados bancários para pagamento:
Banco: _____
Agência: _____ Conta corrente n.º _____ Dígito n.º_____

[LOCAL], [DIA] de [MÊS] de 2024.

Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

MODELO DE DECLARAÇÕES DIVERSAS

(em papel timbrado da licitante)

Ref. Dispensa Eletrônica n° 002/2024 - Processo n° 008/2024

(Nome da Empresa), CNPJ/MF Nº , sediada, (endereço completo) DECLARA para todos os fins de direito, especificamente para participação no processo de contratação direta por dispensa de licitação realizado pela FEMA, o que se segue:

a) está ciente e concorda com as condições contidas no regulamento da Dispensa referenciada e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

b) não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, salvo menor a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição e no inciso V, do art. 68, da Lei 14.133/2021, acrescido pela Lei nº 9.854, de 27 de outubro de 1999;

c) cumpre as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz, conforme orientado pelo art. 92, inciso VXII da Lei 14.133/2021.

d) não está impedida de participar de licitações ou contratar com a Administração Pública, Direta ou Indireta e que não é declarada inidônea pelo Poder Público, de quaisquer esferas da Federação. Não se encontra, nos termos da legislação em vigor, sujeito a qualquer outro fato ou circunstância que possa impedir a sua regular participação na presente licitação ou a eventual contratação que deste procedimento

possa ocorrer, para fins do disposto artigo 156, inc. IV, da Lei nº 14.133/2021, acrescido pela Lei nº 9.854, de 27 de outubro de 1999.

e) não possui sócios ou administradores servidores ou com parentesco até terceiro grau, de servidores e/ou dirigentes desta entidade, que impeçam a contratação desta empresa, nos termos das legislações vigentes aplicáveis;

f) está ciente de que a falsidade na declaração de que trata os itens anteriores sujeitará o licitante às sanções previstas na Lei n° 14.133/2021, e neste Edital.

g) é responsável pela fidelidade e legitimidades das informações e documentos apresentados digitalmente no sistema eletrônico, estando ciente de que a falsidade de qualquer documento ou a inverdade nele contida ficará sujeita às sanções administrativas e judiciais cabíveis.

i) que não possui qualquer dos impedimentos previstos nos §§ 4° e seguintes, todos do artigo 3° da Lei Complementar n° 123/2.006, alterada, cujos termos declara conhecer na íntegra. (§ 2º do art. 4º da Lei nº 14.133/2021).

j) que atende ao Inciso IV do art. 14 da Lei nº 14.133/2021 no que infere ao vínculo de eventuais servidores públicos desse órgão à empresa.

[LOCAL], [DIA] de [MÊS] de 2024.

Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade