Estudo Técnico Preliminar 5/2024

1. Informações Básicas

Número do processo: 00196.004611/2024-62

2. Descrição da necessidade

Estudo para contratação de Serviços Gerenciados e Integrados de Segurança e Serviços de Conectividade Wireless e local, compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança, transferência de conhecimento para a equipe do Cofen e fornecimento de solução de conectividade para rede wireless e local.

Justificativa

Em relação às questões de segurança da informação, é de conhecimento público que diversos órgãos brasileiros são alvos de constantes ameaças, como ataques ao Ministério da Saúde, STF, STJ, TRF 3ª Região, Justiça Federal de SP e MS, etc. Além de instituições financeiras e demais entes privados.

Verifica-se ainda que o Cofen lida todos os dias com elevada troca de informações, além de um grande e complexo volume de dados sensíveis de milhares de cidadãos.

Além disso, em 2020 um novo cenário surgiu em decorrência da Covid-19. Processos de transformação digital das organizações públicas acabou por forçar as organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma, os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente, o que leva à conclusão da necessidade de que as instituições públicas tenham um altíssimo nível de segurança cibernética.

Nestes cenário em que há o avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no tratamento dos riscos de ocorrência de invasões da rede, fato que torna relevante a realização de investimentos em soluções de cibersegurança, fato que motiva a realização destes estudos, que visa a identificação de solução de segurança que possa apoiar o monitoramento da rede e controle de ações internas e identificação de situações suspeitas dentro da rede de computadores do Cofen.

Assim, verifica-se que a estratégia da implementação da segurança da informações em camadas, é adequada, uma vez que consiste na disposição de várias etapas de proteção à operacionalidade do Cofen, de modo a blindar seus arquivos e dados mais sensíveis contra ataques cibernéticos desde a camada física de rede até a camada de aplicações, de forma que a metodologia adotada reforça as fronteiras digitais com vários muros de sustentação de forma gradativa.

Pelo exposto, resta verificada a preocupação da equipe de tecnologia da informação do Cofen em direcionar os investimentos de forma estratégica, promovendo a elevação gradativa dos níveis de segurança institucional e a maturidade das equipes técnicas de forma a alcançar vários benefícios, tais como:

- Proteção contra malwares, ransomware, wannacry, botnet entre outros;
- Proteção contra vazamentos de dados e phishing;
- Segurança ágil e dinâmica;
- Oferece proteção mais forte, multicamadas;
- Controle de ativos; e
- Gerenciamento centralizados dos recursos de rede e segurança, dentre outros citados em cada projeto.

Além disso, o Cofen vivencia uma transformação em sua área de tecnologia da informação, seja atualizando os sistemas legados seja por demanda de novos serviços, com o intuito de ser tornar um órgão com 100% dos seus serviços de forma digital.

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

Sendo assim, se faz necessário a contratação de solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Cofen, tendo como objetivo garantir a segurança e o controle de acesso dos usuários, a rede internet e intranet, permitindo a aplicação de filtros e a identificação de ataques externos e internos.

A Solução Integrada de Serviços Gerenciados de conectividade wireless permitirá ao Cofen a utilização de novas tecnologias como acesso à internet através de notebooks, tablets e celulares, bem como dar maior comodidade e mobilidade aos usuários da rede do Cofen, sendo composta por itens de serviços contínuos em tecnologia da informação e abrangendo todo o ambiente computacional. Também farão parte do escopo atividades relacionadas à transferência de conhecimento e aos serviços técnicos especializados.

A ação visa proteger a rede de ameaças desconhecidas externas, além das internas que podem ocorrer com máquinas infectadas vindo de trabalho híbrido/remoto ou de visitantes.

3. Área requisitante

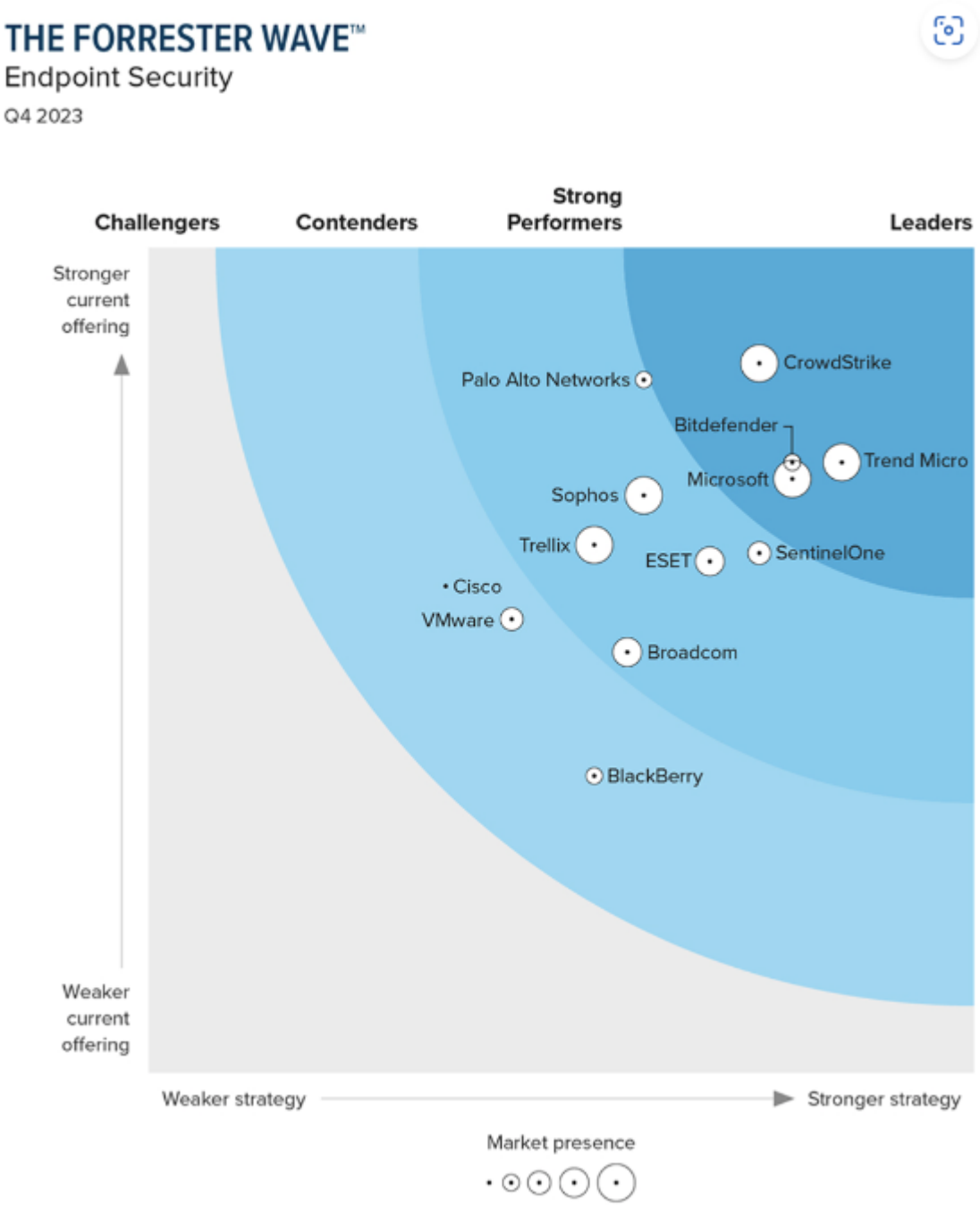
Área Requisitante	Responsável
Departamento de Tecnologia da Informação e Comunicação	Davi Luiz Andrade Lopes Vieira

4. Necessidades de Negócio

- O atual contrato do Cofen já não atende aos requisitos esperados e não há mais atualização tecnológica, devido ao seu encerramento após os 60 meses iniciais. A gama de fabricantes no atual parque também é um fator dificultoso, pois a reduzida equipe precisa manter atualizada e operando os três fabricantes (whatguard, F5 e sophos) de Firewall, WAF, Access Point e Antivírus, que não conversam e não operam de maneira integrada, além do SOC que não atuava de maneira integral em todas as soluções pelo fato da incompatibilidade de comunicação integral entre as soluções existentes. Isso fazia com que a equipe reduzida do Cofen atuasse bem mais tecnicamente do que deveria, para que o órgão pudesse prestar todos os serviços da melhor maneira possível
- Com isso, durante os últimos 5 anos esse fato de não ter uma gerencia centralizada e única, sendo operado por 3 empresas distintas causou grande dificuldade para manter, monitorar, dar respostas e prover segurança.
- De forma comparativa, se o Cofen fosse contratar um profissional com salário médio de R$12.000,00, ele custaria por mês cerca de R$30.000,00 e ao logo dos 5 anos de contrato dessa solução, R$ 1.800.000,00. Ao elaborar esse estudo com a parte de serviços de locação de equipamentos com serviços também prestados pela futura contratada, sem tirar a autonomia do Cofen em operar a solução, seria uma equipe por traz da solução e não dependeríamos de uma única pessoa, sendo a responsabilidade compartilhada com especialistas nas soluções.
- Para uma atuação centralizada e eficaz, assim como ocorre no contrato de nuvem do Cofen, busca-se uma única empresa prestando os serviços elencados neste documento
- Sobre o atual mercado, os quadrantes Gartner e Forrester Wave trazem as seguintes referências para essas soluções, que abarcam as necessidades almejadas:

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (December 2023)



- Sobre os equipamentos de firewall, os quadrantes abaixo exemplifica algumas das soluções existentes:

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (December 2022)

- Das necessidades que pretende-se manter e evoluir, e elencando a análise de soluções e a seleção da opção mais adequada para atingir esses fins organizacionais, cita-se as abaixo:

  a) Proteção das informações sensíveis ao negócio do Cofen;

  b) Aumentar a eficiência da segurança, proteção e autenticidade dos dados e acessos;

  c) Redução da probabilidade de ocorrência de incidentes de segurança;

  d) Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet;

  e) Amplificação da camada de proteção e visibilidade de informações sensíveis;

  f) Fluxo automatizado de descoberta de informações sensíveis em todos os pontos do ambiente;

  g) Garantir a disponibilidade e continuidade dos serviços de TI tanto no datacenter interno quanto no ambiente em nuvem que pode ser aws, azure, google ou huawei (atual contrato).

- Incrementar e otimizar o gerenciamento, a eficiência e a proteção das informações do ambiente tecnológico do Cofen.

- Aprimoramento continuado das ações de Segurança da Informação, objetivando o atendimento à totalidade dos usuários do ambiente tecnológico do Cofen;

- Melhoramento da capacidade de detecção e prevenção de ameaças cibernéticas, comportamentos suspeitos dos usuários, mal-uso dos dados institucionais e vazamentos de dados sensíveis.
- Atualização e modernização do ambiente tecnológico do Cofen, mantendo assim a infraestrutura de rede segura, disponível e plenamente operacional para a disponibilidade de informações precisas e confiáveis à sociedade e aos diversos usuários de seus sistemas, assegurando deste modo o negócio do Cofen.
- Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico, bem como disponibilizar equipamentos, bases de dados e informações precisas e confiáveis.
- Para que se tenha uma padronização de tecnologias, divisão de esforço entre Cofen e Corens, e seguindo a linha da gestão de divulgação dos processos, é importante que o processo seja definido com ARP.
- A iniciativa em questão está em conformidade e encontra-se alinhada ao Plano Diretor de Tecnologia da Informação – PDTIC.

5. Necessidades Tecnológicas

Para garantir a disponibilidade evitando-se que falhas em um equipamento cause a indisponibilidade dos serviços, a solução deverá ser baseada em hardware e software projetados especificamente para o fim objeto desta contratação.

- Os softwares e hardwares que contemplam a solução de TIC devem ser do mesmo fabricante ou, no caso de software/hardware de um outro fabricante/fornecedor, este deverá ser formalmente autorizada e homologada pelos respectivos fabricantes.
- Durante a vigência contratual e o prazo de garantia, o fabricante deve garantir a atualização de patches e softwares de todos os componentes que compõe a solução de TIC, de modo irrestrito e ilimitado.
- A solução deve ser oferecida na última versão disponibilizada pelo fabricante. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Além dos requisitos de negócio e tecnológicos, a presente contratação destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para assegurar o alcance dos objetivos pretendidos com a aquisição, conforme a seguir:

a) A solução deverá ser compatível com as demandas previstas no PCA e PDTIC do Cofen.

b) Observar aspectos de compatibilidade com o datacenter do Cofen e serviços de nuvem do Cofen.

Requisitos de Negócio

- Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico do Cofen, bem como disponibilizar equipamentos, bases de dados e informações precisas e confiáveis.
- Incrementar e otimizar o gerenciamento, a eficiência e a proteção das informações do ambiente tecnológico do Cofen.

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

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

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

Requisitos de Capacitação

- Na elaboração do Projeto Executivo deverá ser detalhado e especificado o treinamento a ser ministrado pela contratada, devendo ser gravado, podendo ser realizado de forma remota e ao menos duas turmas por treinamento, para não interromper as atividades do Cofen.
- Minimamente deverá conter 40h por turma de firewall, 16h por endpoint, 24h por conectividade e 8h por conectividade wireless.

Requisitos Legais

- Lei n.º 14.133/2021 – Lei de Licitações e Contratos Administrativos;

- Lei nº 10.520/2002 - Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

- Decreto nº 11.462/2023 e suas alterações – Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

- Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD);

- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

- Instrução Normativa SLTI/MPOG nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

- Instrução Normativa SEGES/ME n.º 73, de 5 de agosto de 2020 – Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

Requisitos de Manutenção

- O serviço de manutenção, atualização e suporte técnico da solução deverá ser executado pela Contratada e /ou pelo Fabricante durante toda a vigência contratual, a partir da data de emissão do Termo de Recebimento Definitivo referente à implantação e operacionalização da solução no ambiente tecnológico do Cofen, e deverá contemplar obrigatoriamente no mínimo:

  a) Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

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

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

  d) Execução de teste gerais de funcionamento e conectividade;

  e) Execução de configuração de rede e roteamento para as aplicações configuradas;

f) Execução de cópia de segurança (backup) das configurações dos equipamentos;

g) Entrega, por parte da Contratada, de manuais técnicos e/ou documentação dos softwares licenciados em caso de alterações dos mesmos, sem ônus adicionais para o CONTRATANTE;

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

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

Requisitos Temporais

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

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

- Os serviços de fornecimento do objeto – isto é, a execução completa dos serviços e tarefas previstas objetivando a plena e efetiva operacionalização da solução no ambiente do Cofen – deverão ser executados no prazo máximo de até 120 (cento e vinte) dias consecutivos a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

Requisitos de Segurança e Privacidade

- A Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pelo Cofen para execução do Contrato.

- A Contratada deverá assinar Termo de Ciência e Termo de Confidencialidade e Sigilo.

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

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

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

Requisitos Sociais, Ambientais e Culturais

- Requisitos Sociais:

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

- Requisitos Ambientais:

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

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

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

- Requisitos Culturais:

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

Requisitos de Arquitetura Tecnológicas

- Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.
- Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.
- Caberá à Contratada a disponibilização de ferramentas/scripts de retorno imediato ao estado original da estrutura da Contratada caso a instalação e migração dos produtos /softwares da Contratada apresente falha.
- A Contratada realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.
- A Contratada deverá fornecer todas as licenças necessárias de todos os componentes da solução ofertada e dos elementos adicionais que se fizerem necessários à instalação/migração e à perfeita operação do ambiente de produção.

Requisitos de Projeto e de Implementação

- A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do Cofen em no máximo 120 (cento e vinte) dias corridos, a partir da assinatura da Ordem de Serviço.
- Em caso de alterações necessárias nas especificações do projeto original durante a execução dos trabalhos, competirá à Contratada elaborar o projeto da parte a ser alterada e submetê-lo à aprovação do Fiscal, não podendo ocorrer, no entanto, alteração substancial das disposições gerais formuladas pelo projeto original.

Requisitos de Implantação

- Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

a) responsabilizar-se pela completa implantação do projeto, ou seja, todos os custos necessários à operacionalização dos equipamentos;

b) responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes de aceitação;

c) instalar e configurar todos os produtos do fornecimento da solução;

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

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

Requisitos de Garantia e Manutenção

- O prazo de garantia dos serviços, que não envolvam reposição de componentes ou dispositivos, será de 90 (noventa) dias. Caso o serviço tenha que ser refeito dentro deste período, o ônus correrá por conta da Contratada.
- O direito do CONTRATANTE à garantia técnica cessará caso a solução seja alterada pelo próprio ou por fornecedores que não a Contratada e/ou Fabricante responsável pelo serviço em questão.

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

Requisitos de Experiência Profissional

- Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprovem que a licitante já prestou serviços compatíveis em prazo e complexidade com o objeto desta contratação.
- Para a comprovação do atendimento das especificações técnicas dos equipamentos que compõe a solução ofertada, a LICITANTE deverá apresentar, juntamente com sua proposta comercial, documento detalhando as informações, local, site, páginas, documento, etc, necessários para aferição e atendimento de todos os itens da especificação técnica, ou seja, deverá apresentar uma espécie de índice ou planilha ponto-a-ponto, indicando o item, o documento que atende a especificação (nome do mesmo), o local onde está disponibilizado o documento (URL, Site, ou outro disponibilizado de forma digital), a página, e o texto que comprova o atendimento ao item.

Requisitos de Formação da Equipe

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

Requisitos de Metodologia de Trabalho

- A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.
- A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.
- A CONTRATADA deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e via telefônica.

Requisitos de Segurança da Informação e Privacidade

- Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pelo CONTRATANTE, incluindo as Políticas e Diretrizes de Governo, normativos associados ou específicas de Tecnologia da Informação, Política de Segurança da Informação e Comunicações e Normas Complementares do GSI/PR.
- Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia e gerenciamento do prestador de serviços.
- A Contratada deverá credenciar, junto ao CONTRATANTE, seus profissionais autorizados a operar presencialmente (on-site) no sítio do CONTRATANTE e, quando couber, também aqueles que terão acesso aos sistemas corporativos.
- Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.
- Devem ser mantidos registros sobre todas as falhas ocorridas e sobre todas as manutenções executadas.
- A Contratada se compromete a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.
- A Contratada deverá realizar e apresentar ao CONTRATANTE, quando solicitado, uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados ao objeto da contratação, indicando o nível de risco sob o qual o CONTRATANTE está exposto, baseada em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada por este CONTRATANTE.

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

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

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

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

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

  a) Término ou rompimento do Contrato;

  b) Solicitação do Cofen.

Requisitos de Sustentabilidade

- Os serviços deverão ser executados em conformidade com as orientações e normas voltadas para a sustentabilidade ambiental, em especial as contidas no art. 6º da Instrução Normativa/SLTI/MPOG nº 01, de 19 de janeiro de 2010 e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

- Além disso, deverão ser estimuladas as boas práticas de otimização de recursos, redução de desperdícios e menor poluição pautados nos seguintes pressupostos e exigências, quando couberem:

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

b) Economia de energia;

c) Reciclagem de lixo;

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

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

Da Exigência de Carta de Solidariedade

- Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, exclusiva para este certame, que assegure a execução do contrato.

Da Verificação de Amostra do Objeto

- A licitante classificada provisoriamente em primeiro lugar que tiver sua proposta de preços aceita e a documentação de habilitação aprovada poderá, a critério do CONTRATANTE, ser convocada para executar prova de conceito, conforme as regras a serem estabelecidas no Termo de Referência.

Da Garantia de Contratação

- Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 2% (dois por cento) do valor total estimado da contratação.

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

- A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 20 dias úteis após a assinatura do contrato.
- O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações Relevantes para o Dimensionamento/Apresentação da Proposta

- Todas as informações relevantes estão dispostas ao longo deste documento e em seus anexos.

Vistoria

- Dada a complexidade e criticidade dos serviços a serem executados, os licitantes deverão, sob pena de inabilitação, realizar vistoria prévia nas dependências do Cofen, a fim de conhecer seu ambiente tecnológico.
- As vistorias poderão ser realizadas até o último dia útil anterior à data marcada para abertura da sessão pública, no horário das 8h às 12h, com o objetivo de inteirar-se das condições e grau de dificuldade existentes, mediante prévio agendamento pelo e-mail: gtic@cofen.gov.br.
- O agendamento deverá ser solicitado com pelo menos um dia útil de antecedência.
- A vistoria será acompanhada por representante do Cofen, designado para esse fim, o qual visará a declaração comprobatória da vistoria efetuada, que deverá ter sido previamente elaborada pelo licitante em conformidade com o modelo, constante do Termo de Referência, em papel timbrado e assinado por representante legal da empresa.
- No ato da vistoria o licitante receberá informações importantes, tais como:

a) Estrutura de planejamento do Cofen;

b) Estrutura organizacional, competências, número de servidores e demais informações sobre as áreas de tecnologia da informação do Cofen;

c) Política Corporativa de Segurança da Informação do Cofen e normativos correlatos; e

- No ato da vistoria o licitante deverá elaborar previamente em conformidade com o modelo estabelecido em edital, TERMO DE CONFIDENCIALIDADE E SIGILO DO LICITANTE, no qual declarará prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CONTRATANTE reveladas à EMPRESA RECEPTORA em função da vistoria prévia realizada para atendimento deste Termo e entregar o referido Termo assinado ao representante do CONTRATANTE, designado para acompanhá-lo na vistoria.
- Nos termos do §3º do art. 63 da Lei nº 14.133/2021, a vistoria poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

7. Estimativa da demanda - quantidade de bens e serviços

Item	**Descrição**	**Quantidade**	**Meses**	**Valor Unitário mensal**	**Valor Total**
1	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	2	60	R$	R$

2	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	2	60	R$	R$
3	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	2	60	R$	R$
4	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	1	60	R$	R$
5	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	1	60	R$	R$
6	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	1	60	R$	R$
7	Serviços Técnicos Especializados (horas)	600	60	R$	R$
8	Treinamento da Solução de Serviços Gerenciados de Firewall	1	-		
9	Serviços de Solução de proteção para Estações	500			
10	Serviços de Solução de proteção para Servidores	200			
11	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações	500			
12	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para servidores	200			
13	Instalação da solução de Segurança de Endpoints, Detecção e Respostas	500			
14	Instalação da solução de Segurança de Servidores	200			
15	Treinamento da Solução de Endpoints	1	-		
16	Serviços de Conectividade Local	30			
17	Instalação da solução de conectividade Local	30			
18	Treinamento da Solução de Conectividade Local	1	-		
19	Serviços de Conectividade Wireless	80			
20	Instalação da solução de Conectividade Wireless	80			

21	Treinamento da Solução e Conectividade Wireless	1	-		
Valor TOTAL GLOBAL para o LOTE 05					**R$**

8. Levantamento de soluções

Dentre as opções disponíveis para atendimento da demanda, foram identificadas e analisadas as seguintes alternativas:

- Solução 1: Contratação da Solução em forma de *appliance*.
- Solução 2: Contratação da Solução baseada em serviço (SaaS).
- Solução 3: Implantação de uma solução de software livre

9. Análise comparativa de soluções

1. **Solução 1: Contratação da Solução em forma de appliance.**
2.

Descrição: Este modelo prevê a aquisição dos equipamentos, softwares e treinamentos necessários à implantação da solução pela equipe da CONTRATANTE.

3.

Análise da Solução: Nesta alternativa, todos os componentes da solução deverão ser adquiridos, estudados e operados pela equipe técnica da CONTRATANTE.

4.

A situação atual não é ideal, pois a equipe técnica do Cofen, já insuficiente para monitorar adequadamente os incidentes de segurança e atender às demais demandas da autarquia, trabalha em um regime de 8x5 (oito horas por dia, cinco dias por semana), enquanto as ameaças estão ativas em um regime de 24x7 (vinte e quatro horas por dia, sete dias por semana), exigindo claramente um monitoramento contínuo.

5.

Além disso, a "internalização" do processo exige um significativo investimento intelectual (treinamento completo), considerando que o Cofen não tem equipe técnica com a expertise necessária para esse tipo de solução, o que acarretaria um gasto excessivo de tempo, aumento de equipe além do necessário e consequentemente, recursos financeiros.

6.

O atual contrato do Cofen segue esse modelo e é considerável inviável.

1.

Solução 2: Contratação da Solução baseada em serviço (SaaS).

2.

Descrição: Este modelo prevê que a Contratada seja responsável por toda a operação.

3.

Análise da Solução:

Esta solução baseia-se na gestão integral da operação pela Contratada, isto é, a Contratada será responsável por operar continuamente em regime 24x7 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano).

No modelo de contratação proposto, a Contratada deve fornecer todos os equipamentos, licenças de software e profissionais qualificados, os quais devem estar aptos a desempenhar todas as operações conforme o rendimento esperado.

4.

Esta solução baseia-se na contratação de um fornecedor de serviços, que ficará responsável por toda a plataforma operacional a ser integrada ao ambiente tecnológico do CONTRATANTE, garantindo a segurança de todos os ativos de TIC.

Para garantir tal proteção, a plataforma de serviço (Software as a Service – SaaS) deve integrar-se completamente ao ambiente tecnológico do Cofen, abrangendo todos os módulos e componentes, com o objetivo de estabelecer um ambiente uniforme de monitoramento, prevenção, análise, investigação, inteligência, defesa e resposta a incidentes.

O fornecedor deve operar 24 x 7 x 365, contando com processos, equipe de especialistas e ferramentas adequadas para a segurança da informação, seguindo as melhores práticas da Administração e a legislação aplicável, como a ABNT ISSO/IEC 27001, as normas GSI/PR e a Lei Geral de Proteção de Dados (LGPD).

Este modelo é considerado o mais adequado pela Equipe de Planejamento da Contratação, pelas razões apresentadas nas Soluções 1 e 3.

5.

Solução 3: Software Livre

Descrição: Este modelo prevê que a utilização de softwares de código aberto.

6.

Análise da Solução: Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe interna, falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

7.

Solução similar em outro órgão ou entidade da Administração Pública

Nesta seção, analisam-se os aspectos determinados pela IN SGD/ME nº 94/2022 para cada solução a ser considerada em contratações de TIC. Realizou-se uma consulta ao catálogo de Software Público Brasileiro, mas não se identificou nenhuma solução adequada para satisfazer as necessidades de negócio da CONTRATANTE, assim como os requisitos tecnológicos estabelecidos neste Estudo Técnico.

REQUISITO	SOLUÇÃO	SIM	NÃO	NÃO SE APLICA

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X		
	Solução 2	X		
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e	Solução 1			X

funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 2			X
	Solução 3			X

Em conformidade com a Portaria STI/MP nº 46, de 28 de setembro de 2016, declara-se que a solução a ser contratada não se enquadra como Software Público Brasileiro.

10. Registro de soluções consideradas inviáveis

Solução 1: Contratação da Solução como *Appliance*: Conforme as razões elencadas no item anterior, este modelo de contratação se mostrou inviável.

Solução 3: Software Livre: Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

11. Análise comparativa de custos (TCO)

Das três soluções apresentadas, a **Solução 2 - Contratação da Solução baseada em serviço (SaaS)** - foi considerada a melhor alternativa dentre as opções elencadas.

O levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela Instrução Normativa nº 65/2021 da Secretaria de Gestão (SEGES) do Ministério da Economia. Este levantamento servirá para balizar a viabilidade financeira do projeto.

Em atendimento ao art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021:

"Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I. 1. - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;
II. 2. - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
III. 3. - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
IV. 4. - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou UASG 420001 Estudo Técnico Preliminar 3/2023;
V. 5. - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos."

Conforme orienta a referida Instrução Normativa foi realizada pesquisa no Painel de Preços (disponível em https://paineldeprecos.planejamento.gov.br/), que consta no documento: Quadro comparativo de preços

12. Descrição da solução de TIC a ser contratada

Serviços Gerenciados e Integrados de Segurança e Serviços de Conectividade Wireless, compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança, transferência de conhecimento para a equipe e fornecimento de solução de conectividade para rede wireless para o Cofen.

13. Estimativa de custo total da contratação

Valor (R$): 9.849.040,55

Assim, considerando o resultado das pesquisas elencadas anteriormente, temos o valores elencados no quadro de preços

14. Justificativa técnica da escolha da solução

1. Em relação às questões de segurança da informação, é de conhecimento público que diversos órgãos brasileiros são alvos de constantes ameaças, a exemplo o recente ataque ao Ministério da Saúde, onde o hacker atingiu o principal sistema do Ministério; o ataque a Secretaria de Fazenda do Rio de Janeiro, onde foram vazados 420Gb de dados e o ataque ao Sebrae, onde as máquinas virtuais foram atacadas e criptografadas fazendo o site e sistema ficarem fora do ar por vários dias. Além destes, também foram alvo de ataques STF, STJ, TRF 3ª Região, Justiça Federal de SP e MS, etc.
2. Verifica-se ainda que o Cofen lida todos os dias com elevada troca de informações, além de um grande e complexo volume de dados sensíveis de milhares de cidadãos.
3. Além disso, em 2020 um novo cenário surgiu em decorrência da Covid-19. Processos de transformação digital das organizações públicas acabou por forçar as organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente, o que leva à conclusão da necessidade de que as instituições públicas tenham um altíssimo nível de segurança cibernética.
4. Nestes cenário em que há o avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no tratamento dos riscos de ocorrência de invasões da rede, fato que torna relevante a realização de investimentos em soluções de cibersegurança, fato que motiva a realização destes estudos, que visa a identificação de solução de segurança que possa apoiar o monitoramento da rede e controle de ações internas e identificação de situações suspeitas dentro da rede de computadores da CONTRATANTE.
5. Assim, verifica-se que a estratégia da implementação da segurança da informações em camadas, é adequada, uma vez que consiste na disposição de várias etapas de proteção à operacionalidade do Cofen, de modo a blindar seus arquivos e dados mais sensíveis contra ataques cibernéticos desde a camada física de rede até a camada de aplicações, de forma que a metodologia adotada reforça as fronteiras digitais com vários muros de sustentação de forma gradativa.
6. Desta forma as camadas de segurança oferecem uma proteção maior, além de garantir que os criminosos tenham mais dificuldade na hora de tentar invadir um sistema, podendo até mesmo desestimular a tentativa, além disso a estratégia possibilita com que o Cofen possa efetuar a implementação gradativa por meio de contratações de soluções que exigem níveis variáveis de maturidade das equipes.
7. Pelo exposto, resta verificada a preocupação da equipe de tecnologia da informação da CONTRATANTE em direcionar os investimentos de forma estratégica, promovendo a elevação gradativa dos

níveis de segurança institucional e a maturidade das equipes técnicas de forma a alcançar vários benefícios, tais como:
8.

a) Proteção conta malwares, ransomware, wannacry, botnet entre outros;

9.

b) Proteção contra vazamentos de dados e phishing;

10.

c) Segurança ágil e dinâmica;

11.

d) Oferece proteção mais forte, multicamadas;

12.

e) Controle de ativos; e

13.

f) Gerenciamento centralizados dos recursos de rede e segurança, dentre outros citados em cada projeto.

14. Além disso, o Cofen vivencia uma transformação em sua área de tecnologia da informação, seja atualizando os sistemas legados seja por demanda de novos serviços.
15. Desta forma, é essencial viabilizar a proteção adequada e atualizada do seu ambiente computacional (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de programas maléficos que ponham em risco a segurança e a continuidade das atividades.
16. Sendo assim, se faz necessário a contratação de solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Cofen, tendo como objetivo garantir a segurança e o controle de acesso dos usuários, a rede internet e intranet, permitindo a aplicação de filtros e a identificação de ataques externos e internos.
17. A Solução Integrada de Serviços Gerenciados de conectividade wireless permitirá a CONTRATANTE utilização de novas tecnologias como acesso à internet através de tablets e celulares, bem como dar maior comodidade e mobilidade aos usuários da rede do Cofen, sendo composta por itens de serviços contínuos em tecnologia da informação e abrangendo todo o ambiente computacional. Também farão parte do escopo atividades relacionadas à transferência de conhecimento e aos serviços técnicos especializados.
18. A ação visa proteger a rede de ameaças desconhecidas externas, além das internas que podem ocorrer com máquinas infectadas vindo de trabalho híbrido/remoto ou de visitantes.

15. Justificativa econômica da escolha da solução

Conforme demonstrado no item 11 - Análise comparativa de custos (TCO), só existe um tipo de solução viável.

Apesar de não ser uma solução amplamente utilizada para esse tipo de solução, em que pese que o TCU foi inovador e desde meados de 2018 possui contrato de segurança como serviço, a equipe decidiu utilizar apenas os preços de outras licitações, e não levantou preços com fornecedores. Assim, as médias são mais reais e próximas dos padrões já praticados no mercado.

16. Do parcelamento da contratação

Aspectos Técnicos

- Considerando o disposto no inciso I do §2° do art. 12 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a Equipe de Planejamento da Contratação avaliou a viabilidade de *"realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viável e economicamente vantajoso"*.

- O art. 40, inciso V, alínea "b" da Lei nº 14.133/2021, dispõe que:

> *Art. 40 O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:*
>
> *(...)*
>
> *V - atendimento aos princípios:*
>
> *(...)*
>
> *b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso*

- Similarmente, o Tribunal de Contas da União se manifestou sobre o tema através do disposto na Súmula n º 247 de 2007: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade"

- Todavia, nem sempre a licitação com o parcelamento do objeto é a mais eficiente em termos econômicos para a administração, especialmente quando considerados objetos de alta complexidade – o que é o caso da contratação em tela – cite-se como exemplo o Acórdão nº 3.140/2006 – TCU – 2ª Câmara, cujo trecho inerente está transcrito a seguir:

> *"Cabe considerar, porém, que o modelo para a* ***contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços****. Para cada um de cinco prédios, previram-se vários contratos (ar-condicionado, instalações elétricas e eletrônicas, instalações hidrossanitárias, civil). Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão nº 3140/2006 do TCU).*

- Deste modo, para a pretendida aquisição se faz necessário a contratação de **solução única de TIC**, considerando questões técnicas, bem como o ganho de economia em escala, sem prejuízo à ampla competividade, uma vez que existem no mercado várias empresas com capacidade de fornecer soluções que, não obstante possuírem características distintas, atendem ao mesmo objetivo. O agrupamento encontra ainda justificativa em decisões já deliberadas pelo TCU sobre a matéria, tais como, o Acórdão nº 5.260/2011 – TCU – 1ª Câmara, de 28/06/2011, que decidiu que *"Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si".*

- Ademais, em termos administrativos, a adjudicação do objeto desta contratação à Contratadas distintas, além de aumentar o custo administrativo (em ofensa aos princípios da economicidade, razoabilidade e eficiência), oportuniza que as eventuais Contratadas, eventualmente deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra Contratada, originando deste modo uma série de possibilidades e brechas para inconformidades, incongruências e desentendimentos.

- De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade dos serviços de TIC do Cofen para com a sociedade brasileira, é fundamental que o objeto desta contratação seja adjudicado a uma única licitante.

- Neste sentido, conforme exposto, a Equipe de Planejamento da Contratação optou pelo não parcelamento do objeto, e sim pela contratação de solução única, tendo em vista a garantia que a separação em itens distintos compromete técnica e administrativamente a aquisição e gestão do objeto, sendo deste modo

estritamente necessária a aquisição de elementos de forma agrupada, não cabendo assim, o desmembramento do fornecimento.

Aspectos Econômicos

- Conforme dispõe o Inciso I, § 2º, art. 12, da IN SGD/ME nº 94/2022, restou verificado que não é viável particionar o objeto da contratação, uma vez que colocaria em risco o objetivo final desejado. Este não parcelamento da solução gera uma viabilidade econômica trazendo benefícios para a Administração licitante, pois proporciona um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto.

- No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala. Neste sentido, o grupo único é mais satisfatório do ponto de vista da eficiência técnica também, por manter a qualidade da solução de TI, haja vista que o gerenciamento permanece todo o tempo a cargo de um mesmo administrador. Nesse ponto, as vantagens seriam o maior nível de controle pela Administração na execução dos serviços, a maior interação entre as diferentes fases da implantação/implementação, a maior facilidade no cumprimento do cronograma preestabelecido e na observância dos prazos, concentração da responsabilidade pela execução em uma só pessoa e concentração da garantia dos resultados.

- Dessa forma, por suas especificidades, esta contratação ao estar alinhada às práticas de mercado, deverá ter a sua adjudicação da licitação pelo menor preço global. Ademais, o não parcelamento do objeto não restringe a competitividade do certame e nem traz prejuízo ao erário, visto que os itens que compõem o objeto são de mesma natureza e guardam relação entre si.

17. Benefícios a serem alcançados com a contratação

Entre os principais resultados e benefícios a serem obtidos com a implantação da solução a ser contratada, destacam-se:

- Possibilitar o atendimento aos controles e diretrizes previstas na LGPD;
- Mitigação de riscos de segurança da informação associados à exposição, perdas, violações e/ou vazamentos de dados intencionais ou não por usuários do Cofen;
- Diminuição de falsos positivos e negativos;
- Diminuição do tratamento manual de incidentes;
- Aumentar a taxa de automatização de detecção e respostas
- Melhoria da qualidade dos serviços de TIC prestados pelo Cofen à sociedade, com adoção das melhores práticas de mercado relativas à segurança da informação e comunicação;
- Prevenir a ocorrência de incidentes cibernéticos que podem causar impactos à imagem e reputação do Cofen, inclusive o que dispõe a Lei de Proteção de Dados Pessoais;
- Alinhamento estratégico ao PDTIC, garantindo a entrega de valor para que as áreas finalísticas logrem alcançar seus objetivos específicos no âmbito da Missão Institucional do Cofen;
- Ampliar o índice de confiabilidade dos usuários em relação aos serviços prestados pela área de TIC do Cofen, tendo em vista a garantia de segurança destes serviços com a implantação da solução;
- Mitigar internamente os riscos de falhas na segurança dos dados institucionais, bem como identificar, investigar e tratar ocorrências, tendo em vista que a perda, roubo e/ou vazamento de dados do Órgão podem propiciar inúmeros inconvenientes e prejuízos financeiros tanto ao próprio Cofen quanto aos usuários de seus sistemas

18. Providências a serem Adotadas

Infraestrutura Tecnológica

- Disponibilizar conexões físicas e lógicas destinadas ao equipamento a ser instalado.
- Disponibilizar pontos de rede no switch-core para o appliance.

Infraestrutura Elétrica

- Verificar disponibilidade de pontos da rede elétrica para ligação do equipamento.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Diante da necessidade elencada, a equipe considera viável o prosseguimento da contrataç

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

DAVI LUIZ ANDRADE LOPES VIEIRA

Agente de contratação

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Especificao_tecnica.pdf (378.76 KB)

Anexo I - Especificao_tecnica.pdf

Anexo I

Especificações Técnicas

DESCRIÇÃO

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

A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. Os níveis mínimos de serviço contratados, presentes no item "Nível Mínimo de Serviços" destas especificações técnicas, serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.

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

Em suma, o serviço objeto da contratação é subdividido conforme descrito a seguir:

Lote 01 – Solução Integrada de Serviços Gerenciados de Firewall, Endpoints, Conectividade Local e Wireless, sob demanda:

	LOTE 1				
Item	**Descrição**	**Quantidade**	**Meses**	**Valor Unitário mensal**	**Valor Total**
1	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	2	60	R$	R$
2	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	2	60	R$	R$

3	Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	2	60	R$	R$
4	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo A	1	60	R$	R$
5	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo B	1	60	R$	R$
6	Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo C	1	60	R$	R$
7	Serviços Técnicos Especializados (horas)	600	60	R$	R$
8	Treinamento da Solução de Serviços Gerenciados de Firewall (40h para até duas turmas)	)1	-	R$	R$
9	Serviços de Solução de proteção para Estações	500	60	R$	R$
10	Serviços de Solução de proteção para Servidores	200	60	R$	R$
11	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para estações	500	60	R$	R$
12	Serviços de detecção e resposta 24/7, suportado pelo fabricante da solução de proteção para servidores	200	60	R$	R$
13	Instalação da solução de Segurança de Endpoints, Detecção e Respostas	500	60	R$	R$
14	Instalação da solução de Segurança de Servidores	200	60	R$	R$
15	Treinamento da Solução de Endpoints (20h para até duas turmas)	1	-	R$	R$
16	Serviços de Conectividade Local	30	60	R$	R$
17	Instalação da solução de conectividade Local	30	60	R$	R$
18	Treinamento da Solução de Conectividade Local (16h para até duas turmas)	1	-	R$	R$
19	Serviços de Conectividade Wireless	80	60	R$	R$
20	Instalação da solução de Conectividade Wireless	80	60	R$	R$
21	Treinamento da Solução e Conectividade Wireless (16h para até duas turmas)	1	-	R$	R$
Valor TOTAL GLOBAL para o LOTE 01					**R$**

O lote 1 é a junção de todos os itens e poderá ser fornecido por uma única empresa, caso o valor dos itens 16, 17 e 18 sejam inferiores ao lote 2. Nesse caso, a adjudicação do processo licitatório será realizado apenas com a vencedora do lote 1.

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

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

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

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

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

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

O item 16 refere-se aos "Serviços de Conectividade Local", responsável pela conectividade da rede Lan da CONTRATANTE, possibilitando segmentação de redes corporativas e vlans internas.

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

O item 19 refere-se aos "Serviços de Conectividade Wireless", responsável pela conectividade da rede wireless da CONTRATANTE, possibilitando segmentação de redes corporativas e

visitantes, identificação do usuário, controle de qualidade do sinal wifi e implementação de políticas de segurança para rede WAN.

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

Lote 02 – Serviço de Conectividade Local, sob demanda:

LOTE 2					
Item	**Descrição**	**Quantidade**	**Meses**	**Valor Unitário Mensal**	**Valor Total (60 meses)**
1	Serviços de Conectividade Local		60	R$	R$
2	Instalação da solução de conectividade Local		60	R$	R$
3	Treinamento	2	-	R$	R$
Valor TOTAL GLOBAL para o LOTE 02					**R$**

O item 01 do LOTE 02 refere-se aos “Serviços de Conectividade Local”, responsável pela conectividade da rede Lan da CONTRATANTE, possibilitando segmentação de redes corporativas e vlans internas.

O item 02 do LOTE 02 trata dos serviços de instalação referente ao item 01 (Serviços de Conectividade Local), sendo a CONTRATADA responsável por custear todos os equipamentos, softwares, licenças e tudo mais que se fizer necessário tais como demais custos envolvidos na implantação (passagens, diárias e deslocamento de técnicos), de forma a garantir o funcionamento de todas as funcionalidades dos serviços especificados neste Termo.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

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

Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os softwares comerciais deverão, ainda, ser instalados em sua versão

mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

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

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

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

LOTE 01 - Itens 01, 02 e 03 – SERVIÇOS DE PROTEÇÃO DO TRÁFEGO DE REDE DE PRÓXIMA GERAÇÃO (ON PREMISE) com as portas, conexões e cabeamentos disponibilizados pela CONTRATADA, inclusive as SFP e SFP+ com as respectivas gbics)

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

Performance mínima de 12 Gbps de throughput de IPS.

Performance mínima de 6.5 Gbps de throughput para Prevenção de Ameaças.

Performance mínima de 10 Gbps de throughput de NGFW.

Suporte a, no mínimo, 7.000.000 de conexões simultâneas.

Suporte a, no mínimo, 250.000 novas conexões por segundo.

Possuir o número irrestrito quanto ao máximo de usuários licenciados.

Possuir no mínimo 2 (duas) interfaces 10GbE SFP+

Possuir 1 (uma) interface do tipo console ou similar.

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

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

Performance mínima de 5 Gbps de throughput de IPS.

Performance mínima de 3 Gbps de throughput para Prevenção de Ameaças.

Performance mínima de 3,5 Gbps de throughput de NGFW.

Suporte a, no mínimo, 3.000.000 de conexões simultâneas.

Suporte a, no mínimo, 100.000 novas conexões por segundo.

Possuir o número irrestrito quanto ao máximo de usuários licenciados.

Possuir no mínimo 2 (duas) interfaces 10GbE SFP+

Possuir 1 (uma) interface do tipo console ou similar.

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

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

Performance mínima de 2.6 Gbps de throughput de IPS.

Performance mínima de 1 Gbps de throughput para Prevenção de Ameaças.

Performance mínima de 1,6 Gbps de throughput de NGFW.

Suporte a, no mínimo, 1.500.000 de conexões simultâneas.

Suporte a, no mínimo, 55.000 novas conexões por segundo.

Possuir o número irrestrito quanto ao máximo de usuários licenciados.

Possuir no mínimo 1 (uma) interfaces 1GbE SFP.

Possuir 1 (uma) interface do tipo console ou similar.

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

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

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

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

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

O software deverá ser fornecido em sua versão mais atualizada.

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

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

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

A atualização de software deverá enviar avisos de atualização automáticos.

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

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

As notificações deverão ser realizadas via email e SNMP.

Suportar SNMPv3 e Netflow.

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

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

As políticas de NAT deverão ser customizáveis para cada regra.

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

Proteção contra anti-spoofing.

Suportar IPv4 e IPv6.

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

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

Deve possuir tecnologia de conectividade SD-WAN;

Deve implementar balanceamento entre os links WAN com método SpillOver;

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

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

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

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

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

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

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

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

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

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

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

Deve possibilitar o roteamento baseado em VPNs;

Deve suportar criar políticas de roteamento;

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

Interface de entrada do pacote;

IPs de origem;

IPs de destino;

Portas de destino;

Usuários ou grupos de usuários;

Aplicação em camada 7

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

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

Deve suportar Extended VLAN;

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

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

Deve permitir a configuração de jumbo frames nas interfaces de rede;

Deve permitir a criação de um grupo de portas layer2;

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

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

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

Deve possuir otimização em tempo real de voz sobre IP.

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

CONTROLE POR POLÍTICAS DE FIREWALL

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

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

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

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

Controle de políticas por países via localização por IP.

Suporte a objetos e regras IPV6.

Suporte a objetos e regras *multicast.*

PREVENÇÃO DE AMEAÇAS

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

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

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

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

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

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

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

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

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

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

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

Deve ter proteção em tempo real contra novas ameaças criadas.

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

Deve permitir o bloqueio de vulnerabilidades.

Deve permitir o bloqueio de exploits conhecidos.

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

Deve incluir proteção contra ataques de negação de serviços.

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

Suportar bloqueio de arquivos por tipo.

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

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

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

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

Sender Policy Framework (SPF);

Domain Keys Identified Mail (DKIM);

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

Bounce Address Tag Validation (BATV);

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

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

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

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

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

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

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

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

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

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

CONTROLE E PROTEÇÃO DE APLICAÇÕES

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

Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3

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

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

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

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

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

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

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

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

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

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

Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo.

Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

CONTROLE E PROTEÇÃO WEB

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

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

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

Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

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

Possuir pelo menos 90 categorias de URLs;

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

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

Deve ser capaz de forçar as restrições do Youtube;

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

Suportar a criação categorias de URLs customizadas;

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

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

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

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

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

Deve realizar caching do conteúdo web;

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

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

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

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

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

IDENTIFICAÇÃO DE USUÁRIOS

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

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

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

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

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

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

QUALIDADE DE SERVIÇO - QoS

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

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

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

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

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

REDES VIRTUAIS PRIVADAS - VPN

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

Suportar IPsec VPN.

Suportar SSL VPN.

Suportar L2TP e PPTP.

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

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

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

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

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

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

Deve suportar nativamente a integração com a Amazon, afim de estabelecer um túnel seguro entre os appliances e o VPN da AWS. (verificar)

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

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

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

GERÊNCIA ADMINISTRATIVA CENTRALIZADA

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

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

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

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

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

Deve permitir a criação de Templates para configurações.

Deve possuir indicadores do estado de equipamentos e rede.

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

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

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

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

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

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

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

GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

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

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

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

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

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

Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

Deve conter customizações dos relatórios para inserção de logotipos próprios.

Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

Deve permitir a exportação via PDF ou Excel.

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

Deve fornecer relatórios de tendências.

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

Deve possuir mecanismo de procura de logs arquivados.

Deve ter acesso baseado em Web com controles administrativos distintos.

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

SERVIÇOS DE SEGURANÇA DE ESTAÇÕES E SERVIDORES:

CARACTERÍSTICAS GERAIS:

A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

Atualização incremental, remota e em tempo real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

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

Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status; Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais.

Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

O agente anti-vírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;

Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;

Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;

Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;

Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoints e servidores;

Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;

Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

- Proteger o dispositivo com a opção de início de uma varredura;
- Forçar uma atualização naquele momento;
- Ver os detalhes dos eventos ocorridos;
- Executar verificação completa do sistema;
- Forçar o cumprimento de uma nova política de segurança;
- Mover o computador para outro grupo;
- Apagar o computador da lista;
- Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

- Nome do dispositivo;
- Início da proteção;
- Último usuário logado no dispositivo;
- Último update;

- Último escaneamento realizado;
- Status de proteção do dispositivo;
- Grupo a qual o dispositivo faz parte;
- Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;

A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente.

CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO:

Características básicas do agente de proteção contra malwares:

A solução deverá ser capaz de proteger estações de trabalho contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nas estações de trabalho;

Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

Suportar máquinas com arquitetura 32-bit e 64-bit;

O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais macOS 12, 13 e 14 e Microsoft Windows 10 e 11;

Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

Possuir proteção contra exploração de buffer overflow;

Deverá possui atualização periódica de novas assinaturas de ataque;

Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

Deve possuir técnicas de proteção, que inclui:

Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

Algoritimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

Funcionalidade de Antivírus e AntiSpyware:

Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

Capacidade de detectar arquivos através da reputação dos mesmos;

Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

Deverá detectar tráfego de rede para comandar e controlar as estações de trabalho;

Proteger arquivos de documento contra ataques do tipo ransomwares;

Proteger que o ataque de ransomware seja executado remotamente;

Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

Antivírus de Web (verificação de sites e downloads contra vírus);

Controle de acesso a sites por categoria;

Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

Capacidade de verificar somente arquivos novos e alterados;

Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas.

Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

Funcionalidade de detecção de ameaças via técnicas de machine learning;

Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

Funcionalidade de proteção contra ransomwares:

Dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

Dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

Dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação

A solução deverá previnir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

DEP (Data Execution Prevention);

Address Space Layout Randomization (ASLR);

Bottom Up ASLR;

Null Page;

Anti-HeapSpraying;

Dynamic Heap Spray;

Import Address Table Filtering (IAF);

VTable Hijacking;

Stack Pivot and Stack Exec;

SEHOP;

Stack-based ROP (Return-Oriented Programming);

Control-Flow Integrity (CFI);

Syscall;

WOW64;

Load Library;

Shellcode;

VBScript God Mode;

Application Lockdown;

Process Protection;

Network Lockdown.

A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentes para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional,

bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

Funcionalidade de Controle de aplicações e dispositivos:

Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

Oferecer proteção para chaves de registro e controle de processos;

Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

Permitir que todos os dispositivos do mesmo modelo;

Permitir que um único dispositivo com base em seu número de identificação único;

Permitir o acesso total;

Permitir acesso somente leitura;

Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

Funcionalidade de Proteção e Prevenção a Perda de Dados:

Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

Números de cartões de crédito;

Números de contas bancárias;

Números de Passaportes;

Endereços;

Números de telefone;

Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

Lista de e-mails;

Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

Permitir o controle de dados para no mínimo os seguintes meios:

Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

Anexado no navegador (ao menos IE, Firefox e Chrome);

Anexado no cliente de mensagens instantâneas (ao menos Skype);

Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

Funcionalidade de Endpoint Detection and Response (EDR)

A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado; A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

Deve possibilizar o agendamento de consultas (queries);

Deve reter os dados no Data Lake por no mínimo 7 dias.

Funcionalidade de Extended Detection And Response (XDR):

Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

Deve reter os dados no Data Lake por no mínimo 30 dias.

O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação;

Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

Características básicas do agente de proteção contra malwares:

A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

Suportar máquinas com arquitetura 32-bit e 64-bit;

O cliente para instalação em servidores deverá ser compatível com os sistemas operacionais abaixo:

Windows Server 2012;

Windows Server 2016;

Windows Server 2019;

Windows Server 2022;

Debian 8/9/10/11/12;

CentOS 6/7/8;

Oracle Linux 8/9;

Red Hat Enterprise Linux 7/8;

SUSE 12/15;

Ubuntu Server 16.04/18.04/20.04/22.04;

AlmaLinux 8/9;

Rocky Linux 8/9.

Deve possuir integração com as nuvens da Microsoft Azure, Amazon Web Services, Google Cloud e Huawei Cloud para identificar as informações dos servidores instanciados nas nuvens;

Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

Escalação de privilégios dentro de containers;

Programas utilizando técnicas de mineração de criptomoedas;

Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

Detecção de funções internas do kernel que estão sendo adulteradas em um host.

A solução deve também se integrar a tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas.

Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

Possuir proteção contra exploração de buffer overflow;

Deverá possui atualização periódica de novas assinaturas de ataque;

Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

Deve possuir técnicas de proteção, que inclui:

Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

Funcionalidade de Antivírus e AntiSpyware:

Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

Capacidade de detectar arquivos através da reputação dos mesmos;

Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

Deverá detectar tráfego de rede para comandar e controlar os servidores;

Proteger arquivos de documento contra ataques do tipo ransomwares;

Proteger que o ataque de ransomware seja executado remotamente;

Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

Antivírus de Web (verificação de sites e downloads contra vírus);

Controle de acesso a sites por categoria;

Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

Capacidade de verificar somente arquivos novos e alterados;

Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas.

Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

Funcionalidade de detecção de ameaças via técnicas de machine learning;

Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

Funcionalidade de proteção contra ransomwares:

Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.

A solução deverá previnir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

DEP (Data Execution Prevention);

Address Space Layout Randomization (ASLR);

Bottom Up ASLR;

Null Page;

Anti-HeapSpraying;

Dynamic Heap Spray;

Import Address Table Filtering (IAF);

VTable Hijacking;

Stack Pivot and Stack Exec;

SEHOP;

Stack-based ROP (Return-Oriented Programming);

Control-Flow Integrity (CFI);

Syscall;

WOW64;

Load Library;

Shellcode;

VBScript God Mode;

Application Lockdown;

Process Protection;

Network Lockdown.

A solução deverá trabalhar silenciosamente no servidor e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware no servidor.

Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentes para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

Funcionalidade de Controle de aplicações e dispositivos:

Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

Oferecer proteção para chaves de registro e controle de processos;

Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

Permitir que todos os dispositivos do mesmo modelo;

Permitir que um único dispositivo com base em seu número de identificação único;

Permitir o acesso total;

Permitir acesso somente leitura;

Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

Funcionalidade de Proteção e Prevenção a Perda de Dados:

Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

Números de cartões de crédito;

Números de contas bancárias;

Números de Passaportes;

Endereços;

Números de telefone;

Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

Lista de e-mails;

Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

Permitir o controle de dados para no mínimo os seguintes meios:

Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

Anexado no navegador (ao menos IE, Firefox e Chrome);

Anexado no cliente de mensagens instantâneas (ao menos Skype);

Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

Funcionalidade de Endpoint Detection and Response (EDR)

A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado; A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

Deve possibilitar o agendamento de consultas (queries);

Deve reter os dados no Data Lake por no mínimo 7 dias.

Funcionalidade de Extended Detection And Response (XDR):

Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

Deve reter os dados no Data Lake por no mínimo 30 dias.

O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud

Microsoft Azure, Amazon Web Services, Google Cloud, Huawei Cloud, Tencent Cloud e Oracle Cloud;

A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Datalake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação;

Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

OBS: A CONTRATADA deverá fornecer tudo que for necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

Serviços de detecção e resposta 24/7, suportado pela fabricante da solução de proteção para estações e servidores

A CONTRATADA deverá prover serviço de busca, detecção e resposta a ameaças avançadas do Fabricante da solução de segurança ofertada;

Este serviço deve ter funcionamento 24x7 e deve contar com time de especialistas do fabricante da solução das soluções de proteção de estações e servidores ofertada;

Deve disponibilizar (licitante e/ou fabricante) equipes especializadas em no mínimo de 2 SOCs separados geograficamente a fim de manter redundância do serviço;

Deve prover relatórios com resumos das atividades e incidentes de segurança encontrados no ambiente da CONTRATANTE;

Deve prover a verificação da integridade dos componentes da solução de segurança instalada no ambiente da CONTRATANTE;

A solução de MDR deve ser gerenciada na mesma plataforma da solução XDR ou homologada pelos fabricantes distintos demonstrando explicitamente que todas funcionalidades estão disponibilizadas na integração;

A plataforma deverá coletar dados de segurança e telemetria de várias fontes de produtos instalados no ambiente da CONTRATANTE;

Deverá trabalhar com Ferramentas de segurança e serviços de MDR de maneira integrada;

Deve operar sem a necessidade de substituir as ferramentas de segurança existentes;

O Serviço poderá ser fornecido usando ferramentas integradas do fabricante, ferramentas de terceiros ou a combinação dos dois;

Deve proporcionar níveis de serviço personalizados, desde notificação detalhada até resposta a incidentes em grande escala;

Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do fabricante ou homologada pelos fabricantes distintos demonstrando explicitamente que todas funcionalidades estão disponibilizadas na integração;

Deve ser compatível com integrações de terceiros com as seguintes categorias com no mínimo os seguintes fabricantes a seguir:

Firewalls:

- Check Point;
- Palo Alto;
- Fortinet;
- Cisco;
- SonicWall;
- Sophos;
- Watchguard.

Endpoints:

- Microsoft;
- CrowdStike;
- McAfee;
- SentinelOne;
- Check Point;
- Trend Micro;
- Malwarebytes;
- BalckBerry;
- Palo Alto Cortex XDR;
- Sophos.

Provedores de identidade:

- Microsoft Azure IDP, ATA;

- Okta;
- Duo.

Plataformas de filtragem de e-mails:

- Microsoft 365;
- Mimecast;
- Proofpoint.

Infraestrutura de nuvens públicas:

- Amazon Web Services;
- Microsoft Azure;
- Google Cloud;
- Huawei Cloud;
- Tencent Cloud;
- Orca Security;
- Prisma Cloud;
- Oracle Cloud.

Monitoramento de Redes:

- Darktrace;
- Hillstone;
- Forcepoint.

As integrações de terceiros poderão ser via API ou envio de Syslogs.

A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema para uso em nuvem;

O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados, para eventuais consultas;

O serviço de busca, detecção e resposta a ameaças avançadas deverá prover á CONTRATANTE:

Notificações sobre detecções e detalhes das ameaças encontradas no ambiente;

Mitigação de incidentes relacionados a ameaças nos dispositivos cobertos com a solução fazendo a contenção de ameaças: os ataques devem ser interrompidos, evitando a propagação;

Análise de causa raiz realizada para evitar recorrências futuras;

Canais de comunicação com os especialistas do fabricante para sanar dúvidas, dar respostas á incidentes e autorizar mudanças e ações preventivas no ambiente computacional da CONTRATANTE;

IMPLANTAÇÃO DAS SOLUÇÕES INTEGRADAS DE SEGURANÇA

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

Deverão ser apresentados os seguintes entregáveis durante a implantação:

- Fase de Desenho da arquitetura;
- Esquema detalhado de Conexão com dispositivos; e
- Fase de Instalação

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

- Introdução;
- Análise do ambiente;
- Atividades realizadas;
- Configuração de políticas aplicadas;
- Resultados obtidos (Coberturas, eventos de segurança registrados);
- Conclusões;
- Recomendações Específicas;
- Recomendações de Segurança Corporativa
- Introdução;
- Análise do ambiente;
- Atividades realizadas;
- Configuração de políticas aplicadas;
- Resultados obtidos (Coberturas, eventos de segurança registrados);
- Conclusões;
- Recomendações Específicas;
- Recomendações de Segurança Corporativa.

Todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos da CONTRATANTE;

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

A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional da CONTRATANTE, sem prejuízo aos serviços desta;

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

A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executado pela CONTRATADA nos prédios da CONTRATANTE;

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

- Instalação física ou virtual dos equipamentos nas dependências ou no ambiente tecnológico da CONTRATANTE;
- Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sentido de melhorar o gerenciamento e performance e aplicar os "*patchs*" para atualização do sistema, quando necessário;
- Definição das funcionalidades a serem implantadas;
- Definição da parametrização;
- Instalação e configuração de toda a solução com vista ao gerenciamento dos recursos solicitados neste Projeto básico em sua totalidade.

A instalação deve contemplar a verificação da infraestrutura elétrica e lógica existente. Eventuais problemas e necessidade de ajustes devem ser comunicados a CONTRATANTE o qual será responsável pela solução dos mesmos;

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

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

Os serviços de instalação e configuração deverão ser prestados nas dependências da CONTRATANTE.

REQUISITOS GERAIS PARA A PRESTAÇÃO DOS SERVIÇOS

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

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

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

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

O início dos serviços deve ocorrer, obedecendo os prazos dispostos neste termo.

A CONTRATADA da solução deve executar, prioritariamente, como parte obrigatória do processo de instalação e sempre que aplicável a cada solução, as seguintes atividades:

- Definição de políticas e regras de proteção do perímetro "*internet*" visando estar em conformidade com as normas "*ISO/IEC 17799*" e "*NBR-ISO/IEC 17799*", que tratam de segurança da informação e as seguintes configurações;
- Configuração da console de gerenciamento;
- Migração das regras existentes na solução de segurança atual da CONTRATANTE;
- Configuração da autenticação de usuários integrada ao domínio da rede "*Microsoft*", via ferramenta nativa de integração da solução;
- Análise de falsos positivos que podem ser gerados após implantação;
- Adequações pós-instalação;
- Instalação e configuração dos "*firewall's*" em modo "*cluster*" ativo/ativo ou ativo/passivo;
- Instalação e configuração do concentrador de "*logs*", "*archive*" e relatórios;
- Instalação e configuração dos "*gateway's*" "*SMTP*" em modo "*cluster*" ativo/ativo ou ativo/passivo;
- Migração, adequação e definição, juntamente com a equipe de Tecnologia da Informação da CONTRATANTE, das políticas para controle de tráfego de entrada e saída de dados;
- Execução de testes de segurança através da análise de vulnerabilidades completa do perímetro de internet;
- Documentação de todas as configurações realizadas em todas as soluções implantadas;
- Realização de testes, certificação e otimização de todas as soluções implantadas;
- Entrega da documentação de todo o projeto.

LOTE 01 - Item 7: SERVIÇOS TÉCNICOS ESPECIALIZADOS

Item	Descrição	Qtde
7	Serviços Técnicos Especializados (horas)	600

A CONTRATADA deverá disponibilizar, sob demanda, horas de serviços técnicos especializados em segurança da informação, de forma a atender aos seguintes requisitos:

é prevista a utilização média de 600 (seiscentas) horas por ano;

não há garantia de execução das 600 horas, trata-se apenas de previsão estimativa;

os serviços elegíveis a serem executados limitar-se-ão, exclusivamente, aos seguintes casos:

elaboração de pareceres em segurança da informação;

análise de segurança em elementos que não sejam de propriedade da CONTRATADA ou que não estejam no escopo desse projeto;

suporte aos planos de melhoria na infraestrutura de segurança da CONTRATANTE;

suporte a mudanças de arquitetura do ambiente da CONTRATANTE, sobretudo aos aspectos de segurança envolvidos;

avaliação de vulnerabilidades da rede da CONTRATANTE, fora do escopo desse projeto, incluindo a indicação de atualizações ou procedimento necessários para mitigá-las;

apoio na definição e implementação de mecanismos futuros de monitoramento de segurança;

configuração de segurança e atualização de versão de softwares de equipamentos de rede, excluídos os equipamentos de propriedade da CONTRATADA;

orientação quanto a procedimentos de auditoria forense no ambiente computacional da CONTRATANTE;

elaboração, em conjunto com a CONTRATANTE, de planos de conscientização de usuários que proporcionem maior grau de segurança;

mudanças de endereço: incluem-se no escopo dos serviços a desinstalação, o transporte para o novo endereço e a reinstalação de todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços;

transferência de conhecimento às pessoas indicadas pela CONTRATANTE (até seis pessoas por evento), por meio de workshops, conforme as características abaixo:

1. ser realizado nas dependências da CONTRATANTE;
2. ter duração máxima de 8 (oito) horas;
3. ter como conteúdo os conhecimentos referentes a operação, administração, procedimentos e incidentes ocorridos e respectivas ações de mitigação, problemas vivenciados e soluções aplicadas e mudanças de arquitetura ou de tecnologia, além de informações necessárias à transição contratual.

Não serão passíveis de execução por meio de utilização dos Serviços Técnicos Especializados as atividades elencadas nos demais itens e tópicos deste Anexo;

Para a execução dos serviços especificados neste item, a CONTRATADA deverá alocar pelo menos um profissional que detenha comprovação de conhecimento técnico no produto ou serviços a serem prestados, a ser comprovada no momento da assinatura da ordem de serviço.

Condições de execução dos serviços:

os serviços serão executados nas instalações doa CONTRATANTE, por técnicos da empresa CONTRATADA detentores do perfil adequado.

quaisquer serviços ou procedimentos realizados deverão ser previamente aprovados pela CONTRATANTE por meio de Ordem de Serviço, disposto neste Termo, em comum acordo entre o CONTRATANTE e a CONTRATADA, sendo que o tempo necessário ao atendimento deverá ser previamente definido na respectiva Ordem de Serviço;

a prorrogação do prazo de execução de uma Ordem de Serviço somente será possível mediante apresentação, pela CONTRATADA, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pela CONTRATANTE, ou por interesse da CONTRATANTE, em caso de impedimento devidamente justificado que dificulte ou não permita a execução dos serviços;

as ordens de serviço só serão consideradas concluídas após a entrega da documentação dos procedimentos e da configuração resultante nas bases e nos padrões definidos pela CONTRATANTE (incluindo documento as-built);

para recebimento dos serviços será preenchido o Termo de Recebimento de Serviços.

o CONTRATANTE deve avaliar os produtos entregues em até 10 (dez) dias úteis contados da entrega dos serviços/produtos exigidos;

a CONTRATADA deverá reapresentar o material corrigindo eventuais observações feitas pelo CONTRATANTE em até 10 (dez) dias úteis, a contar da comunicação pelo CONTRATANTE;

a cada remessa para avaliação pela CONTRATANTE, a equipe para análise dos produtos da Ordem de Serviço será designada pelo fiscal do contrato e terá prazo de até 10 (dez) dias úteis para análise dos produtos entregues;

caso a CONTRATANTE avalie o material corrigido como insuficiente ou inadequado, a CONTRATADA será considerada em atraso até que sejam sanadas todas as pendências;

estando todos os elementos necessários, a CONTRATANTE fará o recebimento definitivo dos serviços no prazo máximo de 15 (quinze) dias úteis;

estando todos os elementos necessários, a CONTRATANTE fará o recebimento definitivo da ordem de serviço no prazo máximo de 15 (quinze) dias úteis contados do recebimento dos serviços/produtos exigidos;

para a recebimento definitivo será preenchido o Termo de Recebimento de Serviços.

a CONTRATANTE somente autorizará o pagamento das faturas emitidas após o recebimento definitivo dos serviços, realizado mensalmente, de acordo com os níveis mínimos de serviço estabelecidos.

SOLUÇÃO DE CONECTIVIDADE LOCAL e WIRELESS

SERVIÇO DE CONECTIVIDADE LOCAL: O Serviço de conectividade local deve prover no mínimo os seguintes requisitos técnicos:

CARACTERÍSTICAS GERAIS

O serviço de conectividade deverá funcionar através do fornecimento de equipamentos de conectividade local com a disponibilização de switches de 48 portas físicas.

A CONTRATADA deverá fornecer todos os softwares e licenciamentos necessários para atender as funcionalidades do serviço de conectividade local.

A CONTRATADA deverá realizar o gerenciamento centralizado de todos os equipamentos, aplicando configurações e ações em tempo real.

O gerenciamento deverá ser realizado via HTTPS, SSH e REST API;

Possibilitar o agrupamento dos equipamentos, de forma a permitir o gerenciamento de cada grupo de forma individualizada, com seleção de configurações de Vlans para cada grupo de pontos de Acesso.

O gerenciamento poderá estar diretamente e/ou remotamente conectado aos equipamentos por ele gerenciados, ou seja, conectados em diferentes redes e interligados por roteamento.

Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil.

CARACTERÍSTICAS DO SWITCH

Possuir LEDs de identificação de atividades, de status do sistema, de cada porta, e de alimentação;

Possuir altura de no máximo 1U;

Permitir instalação em gabinete de 19″ (dezenove polegadas)

Possuir 48 (quarenta e oito) portas “autosense” ou autonegociável 10/100/1000 com suporte a conectores RJ45 (10BASE-T de acordo com o padrão IEEE 802.3, 100BASE-TX de acordo com o padrão IEEE 802.3U e 1000BASE-T de acordo com o padrão 802.3ab);

Possuir 48 (quarenta e oito) portas full poe nos padrões 802.3af/802.3at;

Possuir, no mínimo, 4 (quatro) portas 10 Gigabit Ethernet com suporte à inserção de transceivers do tipo SFP+;

Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB ou RJ-45.

Capacidade de comutação de no mínimo 176 (cento e setenta e seis) Gbps de throughput;

Possuir capacidade de armazenamento de no mínimo 32.000 (trinta e dois mil) endereços MAC;

Implementar a configuração de no mínimo 256 (duzentas e cinquenta e seis) VLANs simultaneamente;

Implementar a configuração de no mínimo 4.000 (quatro mil) VLANs IDs;

Possuir armazenamento para buffer de no mínimo 2 Mb;

Possuir autenticação 802.1x;

Possuir capacidade de coletar logs via syslog;

Capacidade de aplicar listas ALC;

Capacidade de utilizar IEEE 802.1D MAC Bridging/STP (RSTP compatível);

Capacidade de utilizar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP);

Capacidade de utilizar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP);

Capacidade de utilizar Edge Port / Port Fast;

Capacidade de IEEE 802.1Q VLAN Tagging;

Capacidade de Guest VLAN and Voice VLAN;

Capacidade de IEEE 802.3ad Link Aggregation com LACP;

Capacidade de balanceamento de trafego sobre as portas trunk com Unicast e Multicast;

Capacidade de implementar IEEE 802.1AX;

Capacidade de implementar Spanning Tree Instances (MSTP/CST);

Capacidade de implementar IEEE 802.3x Flow Control and Back-pressure;

Capacidade de implementar IEEE 802.3 10Base-T;

Capacidade de implementar IEEE 802.3u 100Base-TX;

Capacidade de implementar IEEE 802.3z 1000Base-SX/LX;

Capacidade de implementar IEEE 802.3ab 1000Base-T;

Capacidade de implementar IEEE 802.3bz Gigabit Ethernet support;

Capacidade de implementar IEEE 802.3 CSMA/CD;

Capacidade de implementar Storm Control;

Capacidade de implementar Port Mirroring;

Capacidade de implementar DHCP Relay;

Capacidade de implementar autenticação IEEE 802.1x baseado em portas;

Capacidade de implementar IEEE 802.1x Guest VLAN;

Capacidade de implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

Capacidade de implementar IEEE 802.1ab LLDP-MED;

Capacidade de implementar DHCP-Snooping;

Capacidade de implementar MAC Address Filtering

Capacidade de implementar Priority Tag - Packet Ingress Filtering;

Capacidade de implementar QoS usando IEEE 802;

Capacidade de implementar QoS IP TOS/DSCP Based Priority Queuing.

SERVIÇO DE CONECTIVIDADE WIRELESS - O Serviço de conectividade wireless deve prover no mínimo os seguintes requisitos técnicos:

CARACTERÍSTICAS GERAIS

O Sistema de Gerenciamento Centralizado deverá funcionar através de controladora wireless, podendo ser appliance físico, virtual ou em nuvem este deve ser compatível com sistema de servidor virtual VMWare fornecida pela CONTRATANTE.

A CONTRATADA deverá fornecer todos os softwares e licenciamentos necessários para atender as funcionalidades do Sistema de Gerenciamento Centralizado, sem prazo de utilização ou de expiração de qualquer licença.

O sistema de gerenciamento Centralizado da Rede Sem Fio deverá realizar o gerenciamento centralizado de todos os pontos de acesso da rede sem fio, assim como gerenciar a conexão dos usuários conectados em tempo real.

Disponibilizar interface web para a operação da controladora wireless acessível através de protocolo seguro https.

Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados.

Suportar, gerenciar e controlar no mínimo a quantidade de Acess Points adquiridos

Os usuários não autenticados não deverão acessar a mesma Vlan dos usuários autenticados.

Implementar o protocolo IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: PEAP-MSCHAPv2.

Integração com, no mínimo, 02 Servidores Radius que suporte os métodos EAP citados.

Possibilitar o agrupamento de Pontos de Acesso, de forma a permitir o gerenciamento de cada grupo de forma individualizada, com seleção de SSIDs, configurações de Vlans para cada grupo de pontos de Acesso.

O Sistema de Gerenciamento Centralizado poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, ou seja, conectados em diferentes redes e interligados por roteamento. Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração. Possibilitar a criação de um novo SSID, definir os parâmetros de autenticação, definir as políticas de segurança associadas ao SSID, sem qualquer necessidade de acesso individual em cada Ponto de Acesso utilizado

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps Permitir a gravação de eventos em log interno e/ou externo por meio de servidor de SYSLOG da CONTRATANTE Possuir sistema de busca de informações do cliente a partir do endereço IP e endereço MAC.

Possuir Listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC.

Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC.

Opção seleção automática do canal de rádio.

Implementar criptografia entre a comunicação do ponto de acesso e o sistema de gerenciamento centralizado.

Possibilitar, no mínimo, as seguintes formas de autenticação na rede sem fio:

Autenticação por chave pré-compartilhada (PSK), cada estação que se conectar no SSID deverá fornecer a chave pré-compartilhada para acessar os recursos de rede, devendo ser utilizado o protocolo WPA2, com algoritmo de criptografia AES, 128 bits

Autenticação pelo padrão IEEE 802.1X através de autenticação Radius.

Deve possuir funcionalidade de isolar cliente.

Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso

Possuir suporte a pelo menos 8 Vlans com suporte ao padrão IEEE 802.1q

Implementar associação de Regras e de QoS por usuário, com base nos parâmetros da etapa de autenticação. Deve incluir todas as licenças necessárias para que o Ponto de Acesso seja suportado pela solução de gerenciamento

Capacidade de Implementar limitação de banda por usuário.

Possuir VPN-SSL para possibilitar túnel dedicado de criptografia entre dispositivo e controladora.

Possuir VPN-IPSEC para possibilitar túnel dedicado de criptografia entre dispositivo e controladora.

Possuir duplo fator de autenticação OTP para usuários sendo disponibilizado automaticamente ao criar o usuário sem necessidade de licença adicional.

PONTO DE ACESSO

Possuir no mínimo 2(duas) interfaces IEEE 802.3 10/100/1000BaseT;

Suporte a Alimentação PoE (Power over Ethernet) no padrão 802.3at;

Possuir 1(uma) interface console RJ45;

Deve possuir 1 rádio com frequência de 2.4GHz e 1 rádio com frequência de 5GHz;

Suporte a velocidades de no mínimo 1250Mbps em 5GHz e 400Mbps em 2.4GHz;

Cada rádio deverá possuir, no mínimo, 3 antenas internas omnidirecionais, com ganho de, no mínimo, 4.7 dBi para 2.4 GHz e 5.9 dBi para 5 GHz.

Suporte a operação 3x3:3 MU-MIMO;

Possuir, no mínimo, 01(um) Radio Bluetooth low energy (BLE);

Suporte aos padrões IEEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, permitindo o uso simultâneo de usuários configurados em qualquer um dos padrões suportados.

Possuir tecnologia 802.11ac WAVE2;

Suportar a utilização de canais de 20 e 40MHz

Suporte no mínimo 8 SSID’s simultâneos em cada rádio, com configurações independentes.

Possuir LED para a indicação do status de funcionamento do equipamento.

Deve possibilitar a configuração de forma centralizada através de solução de gerenciamento que integre todos os pontos de acesso do ambiente, ou seja, o ponto de acesso receberá todas as configurações da rede sem fios através do sistema de gerenciamento centralizado

Deve permitir a comunicação com o sistema de gerenciamento por IP, sem a necessidade de utilizar a mesma VLAN.

Possuir certificações Anatel, CB, UL, CE, FCC, ISED (IC), RCM, EN 60601-1-2 (Medical Equipment Directive), Plenum-rated (UL2043).

Possuir mecanismo de segurança contra furto do tipo "Kensington security lock point" ou similar.

Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer todos os acessórios para que o serviço de Instalação do ponto de Acesso possa ser realizado.

Injetor de energia

Fornecer alimentação elétrica dos APs via interface de rede 10/100/1000, de acordo com o padrão PoE (Power over Ethernet Plus), mantendo todas as suas funcionalidades e capacidade, calculados para o desempenho máximo do AP, ou seja, todos os transmissores e receptores que compõem o AP;

Os Pontos de Acesso não poderão sofrer nenhum tipo de perda, seja performance, transmissão ou qualquer funcionalidade quando alimentado por Power over Ethernet Plus (PoE) conforme o padrão 802.3af;

Deverá possuir fonte de alimentação com seleção automática de tensão (100– 240 VAC);

Deverá ser específico para ambiente interno;

Deverá fornecer no mínimo 20W;

Deverá ser acompanhado de cabo de energia necessário para sua operacionalização.

INSTALAÇÃO DA SOLUÇÃO DE CONECTIVIDADE LOCAL E WIRELESS

Instalação de equipamentos Access Points e Switches, bem como do software para gerenciamento centralizado destes equipamentos;

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

Deverão ser apresentados os seguintes entregáveis durante a implantação:

- Fase de Desenho da arquitetura
- Esquema detalhado de Conexão com dispositivos
- Fase de Instalação
- Envio de resumo com atividades realizadas, avanços e problemas detectados
- Fase de pós instalação

A CONTRATADA confeccionará relatório(s) final(is) sobre as atividades realizadas e recomendações à CONTRATANTE. Este relatório será entregue 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

- Introdução;
- Análise do ambiente;
- Atividades realizadas;
- Configuração de políticas aplicadas;
- Conclusões;

Todas as atividades envolvidas serão acompanhadas e coordenadas por auditores e técnicos da CONTRATANTE;

A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional da CONTRATANTE, sem prejuízo aos serviços desta;

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

A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executado pela CONTRATADA nos prédios da CONTRATANTE,

Deve abranger a instalação física e lógica da solução, em sua totalidade, com duração máxima de 60 (sessenta) dias corridos, compreendendo, mas não se limitando a essas, as seguintes atividades:

- Instalação física dos equipamentos nas dependências da CONTRATANTE,
- Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sentido de melhorar o gerenciamento e performance e aplicar os “patchs” para atualização do sistema, quando necessário;
- Definição das funcionalidades a serem implantadas;
- Definição da parametrização;
- Instalação e configuração de toda a solução com vista ao gerenciamento dos recursos solicitados neste Projeto básico em sua totalidade;
- Os serviços de instalação e configuração deverão ser prestados nas dependências da CONTRATANTE.

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

É proibida a divulgação de quaisquer aspectos da configuração desses equipamentos, por questões de sigilo e segurança, por parte dos técnicos responsáveis pela instalação e configuração, ou quaisquer outros que tenham acesso a essas informações, salvo quando houver autorização por escrito da CONTRATANTE). Todas as senhas criadas e os usuários cadastrados nos processos de instalação e configuração dos equipamentos devem ser registrados e entregues por escrito ao responsável técnico indicado pela CONTRATANTE.

Deverá ser entregue ao responsável técnico indicado pela CONTRATANTE, relatório com todos os procedimentos e configurações executados, assinado pelo responsável técnico da CONTRATADA.

O início dos serviços deve ocorrer, no máximo, em 72 (setenta e duas) horas úteis, contadas a partir da assinatura do contrato.

A CONTRATADA da solução deve executar, prioritariamente, como parte obrigatória do processo de instalação, as seguintes atividades:

- Configuração da console de gerenciamento;
- Migração das regras existentes na solução de segurança atual da CONTRATANTE;
- Configuração da autenticação de usuários integrada ao domínio da rede "Microsoft", via ferramenta nativa de integração da solução;
- Análise de falsos positivos que podem ser gerados após implantação;
- Adequações pós-instalação;
- Instalação e configuração do concentrador de "logs", "archive" e relatórios;
- Migração, adequação e definição, juntamente com a equipe de Tecnologia da Informação da CONTRATANTE, das políticas para controle de tráfego de entrada e saída de dados;
- Execução de testes de segurança através da análise de vulnerabilidades completa do perímetro de internet.

SERVIÇOS DE TREINAMENTO

Quando solicitado pela CONTRATANTE deverá ser realizado treinamento para repasse de conhecimento à equipe do COFEN contemplando no mínimo:

- Práticas de gerenciamento e troubleshooting da solução instalada;
- Material didático de cada solução implementada.;
- Para no máximo 10(dez) participantes por turma, e até duas turmas.

A CONTRATANTE, cederá somente a sala, os computadores e o datashow (projetor) para o curso, podendo ser ministrado de forma remota.

Todos os custos referentes ao repasse de conhecimento deverão está incluso no valor global do contrato.

SERVIÇOS COMUNS à solução Integrada de Segurança

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

Os serviços deverão observar os seguintes requisitos mínimos, sempre que aplicável a cada uma das soluções adquiridas pela CONTRATANTE:

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

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

Mapear e executar os processos de resposta dos incidentes de segurança ocorridos e documentar na base de conhecimento da CONTRATANTE;

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

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

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

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

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

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

Realizar o ajuste fino (tunning) de toda a solução, adequando-a ao ambiente da CONTRATANTE, e às customizações de configuração necessárias para atender às necessidades da CONTRATANTE;

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

Monitorar os sites WEB da CONTRATANTE, contra pichação (defacement) e ataques, tais como cross-site scripting, SQL injection e DoS;

Monitorar servidores e alerta para mudança em arquivos de configuração; • Executar inventários contendo as informações abaixo:

1. Tipo de computador: servidor, estação ou outra classificação;
2. Sistema operacional;
3. Service pack aplicado;
4. MAC Address;
5. Portas TCP e UDP ativas.

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

acessos indevidos;

Instalação de códigos maliciosos;

Indisponibilidade dos serviços (DoS e DDoS);

ataques por força bruta;

exploração de vulnerabilidades.

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

Será permitida a prestação dos serviços por meio de:

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

Caso seja necessária a utilização de elementos adicionais para o estabelecimento da VPN, estes devem ser alocados pela CONTRATADA.

Avaliar periodicamente a customização dos softwares de gerência da CONTRATADA, incluindo os alarmes de todos os componentes da e ajusta as suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas no console de gerência;

Possibilidade do acesso remoto a interface de monitoramento;

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

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

Caso houver elementos instalados nas dependências CONTRATANTE, estes devem:

possuir fonte de alimentação 110/220V;

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

SERVIÇOS COMUNS À SOLUÇÃO de Conectividade Local e Wireless)

Os equipamentos, produtos, peças ou softwares necessários à prestação dos Serviços de conectividade wireless deverão ser instalados no ambiente da CONTRATANTE, sob demanda em lotes mínimos de 10 access points e switches.

Os serviços deverão observar os seguintes requisitos mínimos:

Serão realizados em todos os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço, em regime 24x7 (24 horas por dia, sete dias por semana);

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

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

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

Executar atividades de suporte, manutenção e resolução de problemas e de configuração, de cada um componentes dos serviços, remotamente;

Realizar o ajuste fino (tunning) de toda a solução, adequando-a ao ambiente da CONTRATANTE e às customizações de configuração necessárias para atender às necessidades da CONTRATANTE;

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

Será permitida a prestação dos serviços por meio de:

1. Estabelecimento de VPN em links Internet alocados pela CONTRATADA exclusivamente para essa conexão ou estabelecimento de VPN em links SLDD alocados pela CONTRATADA exclusivamente para essa conexão;
2. Caso seja necessária a utilização de elementos adicionais para o estabelecimento da VPN, estes devem ser alocados pela CONTRATADA.

Avaliar periodicamente a customização dos softwares de gerência da CONTRATADA, incluindo os alarmes de todos os componentes da e ajusta as suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas no console de gerência;

Os elementos instalados nas dependências da CONTRATANTE, estes devem:

possuir fonte de alimentação 110/220V;

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

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

PLANEJAMENTO, CUSTOMIZAÇÃO DE AMBIENTE E INSTALAÇÃO DE ATIVOS DE REDE

A CONTRATADA deverá atender as seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente, migração tecnológica e ativação de serviços, sem ônus adicionais a CONTRATANTE:

serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para aprovação pela CONTRATANTE;

caso os produtos alocados venham a substituir solução existente na CONTRATANTE, caberá à CONTRATADA levantar a configuração atual e fazer a migração das configurações existentes para a solução utilizada no provimento dos serviços;

a CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se pertinente, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;

as visitas poderão ser realizadas nos dias úteis, das 08:00h as 14:00h, mediante agendamento prévio com a unidade responsável;

Independentemente da alocação dos racks pela CONTRATADA, esta deverá efetuar a reorganização dos racks existentes, de forma a acomodar os seus equipamentos;

As atividades de migração e mudanças deverão ocorrer de acordo com as políticas adotadas pela equipe técnica da CONTRATANTE;

as reuniões de Migração e Mudanças serão realizadas por meio de um reuniões, com periodicidade semanal;

nessas reuniões serão aprovadas ou vetadas mudanças no ambiente operacional que por ventura venham a causar indisponibilidade ou impactos no desempenho dos serviços de TI;

das reuniões, participaram servidores da CONTRATANTE responsáveis pela disponibilização e manutenção da infraestrutura de TI da CONTRATANTE;

na ocasião das reuniões de Migração e Mudanças, deverá participar o técnico responsável pelas atividades da CONTRATADA, para exposição dos riscos associados.

A elaboração do Projeto Executivo estará a cargo da CONTRATADA e deverá atender as seguintes condições:

conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase, respeitando os prazos;

detalhar a ementa dos treinamentos a serem ministrados.

Os equipamentos, softwares e demais componentes necessários à correta prestação dos serviços deverão:

ser entregues, instalados e configurados nas dependências da CONTRATANTE;

conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da CONTRATANTE, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;

conter a última versão de software e firmware disponibilizada pelo fabricante;

ter configuradas senhas de acesso para que a equipe de servidores designados pela CONTRATANTE, efetue o acesso para a visualização das configurações e logs;

ter configurada senha com direitos totais de administração e configuração a ser utilizada pela CONTRATANTE, em caso de emergência;

ser configurados para enviar logs para as soluções de concentração de logs disponibilizados no site central e de contingência da CONTRATANTE;

ser configurados para gerenciamento SNMP versões 1 e 2 por meio da solução em uso na CONTRATANTE;

para aprovação da instalação e configuração de qualquer item que enseje a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

as atividades quando realizadas no ambiente de produção poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 18:00 h, ou em finais de semana e feriados.

Após a instalação, a CONTRATADA deverá realizar operação assistida para os serviços contratados; A operação assistida deverá obedecer aos requisitos abaixo:

iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pela CONTRATANTE, que seja feita em data diferente;

será executada nas dependências da CONTRATANTE, em horário de expediente deste;

caso seja necessária a consecução de atividades, pelo técnico responsável pela operação assistida, que possam afetar a disponibilidade de serviços de rede da CONTRATANTE, estas devem ocorrer após as 18:00h;

caso a CONTRATANTE, encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade da Rede da CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

A CONTRATADA deverá implementar e documentar para todos os componentes da solução as configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários-padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.

REQUISITOS GERAIS PARA A PRESTAÇÃO DOS SERVIÇOS

A CONTRATADA deverá observar aos seguintes requisitos mínimos gerais para a prestação dos serviços, sem ônus adicionais ao CONTRATANTE:

a CONTRATADA será responsável por obter as assinaturas nos respectivos termos de seus funcionários, terceirizados, parceiros ou quaisquer outras pessoas que venham executar serviços integrantes do objeto desta contratação;

o Termo de Confidencialidade e Sigilo determina que a propriedade intelectual de todos os produtos ou conhecimentos gerados advindos da prestação dos serviços pertencem a CONTRATANTE.

Os produtos utilizados para a prestação dos serviços devem:

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

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

Todos os recursos necessários à configuração e administração dos equipamentos, softwares ou quaisquer outros componentes da solução fornecida deverão ser instalados na CONTRATANTE, e estar disponíveis mesmo com a perda de comunicação com a central de monitoramento e gerência da CONTRATADA;

Quaisquer agentes ou certificados digitais necessários à perfeita consecução dos serviços devem ser alocados pela CONTRATADA, sem ônus adicional a CONTRATANTE;

A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando tenham sido causados por seus profissionais durante a execução dos serviços;

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

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

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

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

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

assinaturas de atualização de equipamentos;

atualização de versão de software;

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

serviços gerenciados de segurança;

requisitos que exijam execução de atividades por parte de funcionários da CONTRATADA.

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

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

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

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

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

As atividades, quando realizadas no ambiente de produção, poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 18:00horas, ou em finais de semana e feriados);

No momento de abertura do chamado, deverá ser fornecido a CONTRATANTE, um número único de identificação e deverão ser classificados conforme a Tabela – Atividades Operacionais de Segurança, contida no item – Nível Mínimo de Serviços. A classificação do chamado está sujeita a alteração pela CONTRATANTE, sempre que este julgar necessário. Neste caso, os tempos de atendimento e resolução (NMS) serão contados a partir do momento em que a CONTRATANTE, efetue a solicitação de alteração de prioridade;

Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema para controle de chamados da CONTRATADA;

Os chamados abertos somente poderão ser fechados após autorização da CONTRATANTE;

A CONTRATADA deverá realizar os devidos escalonamentos de acordo com a criticidade e nível de atendimento do incidente ou problema reportado pela CONTRATANTE ou pelo sistema de monitoração;

Após resolução de um chamado técnico, a empresa CONTRATADA deverá encaminhar a CONTRATANTE, relatório contendo descrição do chamado aberto, procedimento de resolução adotado e outros adicionais que poderão ser executados para que o problema ocorrido não se repita; A CONTRATADA deverá fornecer mensalmente, em meio magnético ou eletrônico, os relatórios abaixo descritos:

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

dados, informações, indicadores e métricas que permitam quantificar o percentual de disponibilidade da central de atendimento da CONTRATADA, detalhados para a central de atendimento telefônico e para o portal na Internet;

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

inventário lógico dos ativos;

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

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

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

1. utilização de CPU e memória de todos os itens;
2. utilização de recursos diversos (discos, cache, rede etc);
3. disponibilidade de cada item;
4. atualizações de software realizadas no período;
5. total de chamados cadastrados por item;
6. classificação do chamado pelas prioridades estabelecidas;
7. tempo de atendimento por cada chamado aberto;
8. comprovação de que todos os softwares comerciais estão cobertos por contratos de suporte e atualização de versão e que todos os hardwares alocados estão cobertos por garantia do fabricante.