Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ETICE
Fls. 63

Chamada de Oportunidade de Serviços de Nuvem Pública Nº 001/2023, aderente ao Edital de Pré-qualificação Permanente de Serviços em Nuvem Nº 001/2019 - ETICE

Agosto/2023

1. OBJETO

Chamada de oportunidade para prestação de serviços compreendendo o provimento de recursos em nuvem, para futuras e eventuais contratações de solução de proteção, gestão, avaliação de postura e conectividade para nuvens públicas e privadas, incluindo respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7, contemplando utilização de soluções de nuvem homologadas, de acordo com as especificações e quantitativos previstos neste termo.

2. OBJETIVOS:

Contribuindo com o aprimoramento tecnológico dos entes da Administração Pública do Estado do Ceará e reforçando sua missão de ser referência nacional como empresa de Tecnologia da Informação e Comunicação – TIC, indutora da inovação e modernização para o desenvolvimento econômico-social no fornecimento de serviços de tecnologia de alta performance em nuvem, a ETICE deseja selecionar, dentre as empresas pré-qualificadas, **serviços técnicos especializados para provimento de solução em nuvem**, conforme detalhamento técnico constante neste documento.

Assim, considerando as premissas estabelecidas no Edital de Pré-qualificação 001/2019, a Empresa de Tecnologia da Informação do Ceará – ETICE convoca as empresas pré-qualificadas para que apresentem propostas para fornecimento dos serviços em nuvem, seguindo as definições técnicas deste documento convocatório.

Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX.

Outrossim, vale destacar que os itens de serviços vencedores de cada chamada de oportunidade já serão trazidos para a composição do Marketplace da ETICE, devendo o(s) contrato(s) serem realizados por demanda; ou seja, SEM comprometimento do Orçamento da ETICE, podendo haver a contratação parcelada do objeto da presente chamada de Oportunidade; tudo consoante ao disposto nos itens 13.11, 17.1.1, 17.1.2 e 17.1.3 do Edital de Pré-qualificação, in verbis:

> "13.11. **Os itens de serviços vencedores de cada chamada de oportunidade serão trazidos para a composição dos serviços do marketplace da Etice**, devendo seus preços finais serem mantidos como máximos por um prazo mínimo de 12 (doze) meses a contar da data da homologação do resultado da chamada de oportunidade. (...)
> 17.1.1. Consoante o disposto no art. 140, parágrafos 4º e 5º do Regulamento de Licitações e Contratos da Etice, **fica desde já a ETICE autorizada a celebração de contratos por demanda**.
> 17.1.2. A ETICE fixará um quantitativo ou valor máximo de fornecimento ou serviço a ser utilizado no prazo de vigência do referido contrato, **SEM comprometimento do Orçamento da Etice**.
> 17.1.2. Na hipótese do item anterior, a ETICE **demandará o objeto de forma PARCELADA e apenas quando necessitar, nos termos e prazos definidos no Edital e contrato**, remunerando o contratado apenas pelo que for efetivamente executado." (grifou-se)

Este documento descreve as características funcionais, premissas técnicas e de serviços que deverão ser consideradas pelas pré-qualificadas, para que, munidos de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições preestabelecidas no Edital de Pré-qualificação supracitado.

3. SOBRE O MODELO DE CONTRATAÇÃO

3.1. Esta chamada de oportunidade obedecerá ao disposto no Edital de pré-qualificação de nuvem nº 001/2019 da ETICE e seus anexos, nos Termos de Pré-Qualificação e no Regulamento deLicitações e Contratos da ETICE; sendo regido, também, pela Lei Federal 13.303/2016, pelos Princípios da Direito Civil e, no que couber, pelos Princípios da Administração Pública e demais legislação correlata.

3.2. A chamada será feita em lote único, visto que os itens desta chamada são intrinsecamente interconectados, o que impossibilitaria sua divisão.

3.3. Justificativa de escolha dos recursos em nuvem para provimento dos serviços de Gestão de TI:

3.3.1. Considerando a quantidade de demanda de clientes ETICE para utilização de recursos em nuvem para a gestão e operação de serviços de TI, segurança da infraestrutura de TI, e orquestração de workloads;

3.3.2. Considerando a necessidade de expansão dos itens disponíveis no *marketplace* da ETICE para que seja possível ofertar soluções de gestão e operação dos serviços de TI, capaz de se integrar à diversidade de tecnologias (softwares, aplicativos e plataformas) que são empregadas nas instituições, cada uma com suas particularidades.

3.3.3. Considerando que existem soluções robustas e integradas de gestão e operação dos serviços de TI, aderentes às práticas definidas no ITIL V4 e pertencentes ao quadrante "líderes" do quadrante mágico do Gartner de Gestão de Serviços de TI.

3.3.4. Considerando que o Edital de Pré-qualificação proporcionou a pré-qualificação de diversas empresas, as quais representam diversos fabricantes de soluções, a decisão é pela publicação da chamada não nominada, tendo em vista a possibilidade de contarmos com maior concorrência entre os interessados que atendam as especificações técnicas.

3.4. Assim sendo, a presente chamada de oportunidade será aberta para oferta dos recursos em nuvem, para expandir o catálogo de produtos disponíveis no referido marketplace com a adição dos novos itens definidos nesta chamada.

4. ORIENTAÇÕES GERAIS

4.1. Prazos

Número do Evento	Evento	Prazo limite
1	Recebimento de propostas das empresas pré-qualificadas pela ETICE	8 (oito) dias úteis (*)
2	Pedidos de Esclarecimentos	**Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.**
3	Resposta aos Pedidos de Esclarecimentos	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimentos (**).
4	Pedidos de Impugnação	**Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.**

5	Respostas à Impugnação Interposta	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimento.
6	Avaliação, Negociação e definição da proposta vencedora pela ETICE	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de propostas.
7	Interposição de Recurso	Até 5 (cinco) dias úteis, contados a partir da divulgação da proposta vencedora.
8	Apresentação de Contrarrazões ao Recurso	Até 5 (cinco) dias úteis, contados a partir do término do prazo de interposição de recurso.
9	Decisão **definitiva** da Comissão	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de contrarrazões recursais, podendo variar em razão da complexidade da matéria.
10	Homologação e Adjudicação	Até 5 (cinco) dias úteis, a contar da divulgação da decisão definitiva da Comissão.

(*) O prazo será contado a partir do primeiro dia útil seguinte à publicação deste documento no website da ETICE, no link https://www.etice.ce.gov.br/projeto/pre-qualificacao-permanente/.
(**) O prazo poderá ser alterado conforme disposto no item 5.4.
(***) Caso haja desistência expressa do Prazo Recursal (e consequente Contrarrazões), o Prazo para apresentação da Decisão Definitiva poderá ser reduzido, conforme o caso.

4.1.1. Os Prazos dispostos no item acima poderão variar em conformidade com o caso concreto, **podendo inclusive serem mitigados**, em razão de não apresentação de recursos ou mesmo que as empresas Pré-qualificadas declinem, formalmente, do direito recursal (e consequentes contrarrazões).

4.2. Sobre o envio da Proposta Técnica.

4.2.1. Em razão do período delicado de Pandemia mundial que estamos passando, e até mesmo como um mecanismo de evitar o trânsito de papel e aglomeração de pessoas,consoante previsão disposta no item 13.8.2 do Edital nº, 001/2019 de Pré-Qualificação, a **proposta deverá ser enviada de forma eletrônica e deverá ser CRIPTOGRAFADA utilizando o algoritmo de criptografia AES-256 (FIPS PUB 197).**

4.2.2. A proponente é responsável por gerar uma chave aleatória de 256 bits e manter completo sigilo desta chave, sem revelá-la a terceiros, nem à Etice, até que se tenha passado o período de recebimento de propostas estabelecido na tabela do item 4.1.

4.2.3. Antes ou após criptografada utilizando-se o algoritmo AES-256, a proposta deve ser assinada digitalmente, conforme o modelo da Medida Provisória 2.200-2/2001.

4.2.4. Com o objetivo de facilitar a submissão de propostas e considerando que vários softwares possibilitam a assinatura digital de um documento antes de uma encriptação e não após ela a ETICE aceitará também propostas que tenham sido assinadas digitalmente antes de terem sido encriptadas contanto que o nome do arquivo de proposta possibilite a identificação clara do proponente.

4.2.5. A proposta criptografada e assinada deve ser enviada para o e-mail **avaliacao.nuvem@etice.ce.gov.br. O HORÁRIO DE RECEBIMENTO DAS PROPOSTAS SERÁ ATÉ ÀS 17H (DEZESSETE HORAS) DO ÚLTIMO DIA ÚTIL PARA RECEBIMENTO DAS PROPOSTAS.**

4.2.6. Uma proposta só será considerada **entregue no prazo** caso a Etice responda com ume-mail para o proponente reconhecendo o recebimento dentro do prazo.

4.2.7. A resposta da Etice será assinada digitalmente ou de outra forma por ela estabelecida.

4.2.8. Proposta enviada para e-mail não correto ou com erro de escrita ou que tenha sido recusada pelo servidor não será considerada entregue no prazo.

4.2.9. A proponente deverá enviar a chave criptográfica usada para encriptar a proposta com o algoritmo AES-256 para a Etice em **até 1 (um) dia útil** após encerrado o prazo de recebimento de propostas.

4.2.10. Arquivo corrompido ou chave que não permita descriptografar a proposta fará a proposta nula.

4.2.11. Todos os recursos e serviços necessários deverão ser lançados nas propostas em modalidade OPEX e em moeda nacional (reais).

4.2.12. Na proposta deverá constar as cotações de todos os itens de serviços especificados neste documento, expressas em reais e em valores mensais e anuais.

4.2.13. Para fins de elaboração de Propostas, as empresas participantes deverão considerar que o prazo contratual será de 12 (doze) meses, prorrogável na forma da lei.

4.2.14. A Etice descriptografará todas as propostas válidas e ordenará tais propostas baseadas em seu valor global.

4.3. Processo de Seleção e Negociação

4.3.1. A seleção e negociação da melhor proposta só ocorrerá se existirem, no mínimo,3 (três) propostas válidas para a chamada.

4.3.2. O processo de seleção e negociação respeitará as regras do edital de pré-qualificação e da presente chamada, com base na proposta mais vantajosa para a Etice, de forma a não comprometer a economicidade.

4.3.3. Serão **DESCLASSIFICADAS** as Propostas que:

4.3.3.1 Contenham vícios insanáveis;

4.3.3.2 Descumpram especificações técnicas constantes desta Chamada de Oportunidade;

4.3.3.3 Apresentem preços manifestamente inexequíveis;

4.3.3.3.1 Será considerada inexequível as propostas:

4.3.3.3.1.1 Cujo valor total seja igual ou inferior a 50% do valor estimado para contratação.

4.3.3.3.1.2 Cujo valor do item da proposta seja igual ou inferior a 50% do valor estimado para aquele item.

4.3.3.4 Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE;

4.3.3.4.1.1 A Etice comprovará a exequibilidade das propostas por meio dos itens abaixo:

4.3.3.4.1.1.1 Nota fiscais, faturas, relatórios e medições de serviços semelhantes prestados, dentre outros.

4.3.3.5 Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes;

4.3.3.6 A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada;

4.3.3.7 A desclassificação será sempre fundamentada.

4.3.4 A negociação se dará mediante questionamentos da Etice às empresas titulares de propostas válidas por descontos percentuais que estas possam oferecer em suas respectivas propostas.

5. ESCLARECIMENTOS

5.1. As dúvidas na interpretação do presente documento e anexos, consultas ou pedido de esclarecimentos acerca das informações técnicas porventura existentes, poderão ser feitos via e-mail de forma expressa, clara, concisa e objetiva, constando no corpo do texto do e-mail a identificação completa da empresa pré-qualificada participante e do representante que questiona as informações ou solicita esclarecimentos.

5.2. Os pedidos de esclarecimentos deverão ser encaminhados **até às 17h do 3º (terceiro) dia útil que antecede o término do prazo de apresentação das propostas.**

5.3. O endereço de e-mail para os esclarecimentos é: **avaliacao.nuvem@etice.ce.gov.br.**

5.4. A Etice terá um prazo de até 02 (dois) dias úteis para resposta, sendo possível estender esse prazo de acordo com a complexidade dos esclarecimentos e/ou a necessidade de utilização de recursos técnicos externos à Etice.

5.5. Caso a(s) resposta(s) dos esclarecimentos provoquem alterações das definições técnicas do projeto e estas sejam consideradas relevantes pela Etice, será reiniciada a contagem dos prazos estabelecidos no item 4.1 deste documento, cabendo comunicação prévia e única a todas as pré-qualificadas.

5.6. As quantidades aqui mencionadas são previsões e NÃO implicam em obrigatoriedade de contratação de quaisquer quantidades pela Administração Pública, servindo apenas como referencia para a elaboração das propostas das empresas pré-qualificadas pela ETICE.

6. ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS

6.1. Seguem os itens a serem fornecidos pela pré-qualificada a ser contratada. A lista de serviços computacionais em nuvem indica a quantidade prevista de uso, e servem como referência para o cálculo mensal e para o valor global do contrato, além de referência para o cálculo de valores a serem pagos pela Contratante.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD
1	SOLUÇÃO DE NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA OU NUVEM PRIVADA	LICENÇA	40
2	SOLUÇÃO DE AUTOMAÇÃO DE GOVERNANÇA, POSTURA E CONFORMIDADE PARA NUVENS PÚBLICAS	LICENÇA	8
3	SOLUÇÃO DE PROTEÇÃO PARA APLICAÇÕES WEB EM NUVEM (WAF), DEFESA DE API E AUTOMAÇÕES (BOTS)	PACOTES DE 100 MILHÕES DE REQUISIÇOES	30

4	SOLUÇÃO PARA ANÁLISE DE SEGURANÇA EM DESENVOLVIMENTO DE CÓDIGO FONTE	PACOTES DE 25 DEVELOPERS	20
5	SOLUÇÃO DE ANÁLISE E GESTÃO INTELIGENTE DE VULNERABILIDADE PARA RECURSOS DE NUVEM	PACOTES DE 300 ATIVOS	10
6	SOLUÇÃO PARA INSPEÇÃO DE TRÁFEGO E ACESSO SEGURO À INTERNET	LICENÇA	5.000
7	SOLUÇÃO DE MONITORAMENTO DE EXPERIÊNCIA CONTÍNUA DOS USUÁRIOS	LICENÇA	5.000
8	SOLUÇÃO PARA ACESSO SEGURO A APLICAÇÕES PRIVADAS	LICENÇA	5.000
9	SOLUÇÃO DE SEGURANÇA DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM	LICENÇA	1.000
10	SOLUÇÃO DE PROTEÇÃO E SEGURANÇA DE DADOS	TERABYTE (TB)	300
11	SOLUÇÃO DE PROTEÇÃO PARA AMBIENTES COLABORATIVOS	PACOTES DE 500 USUÁRIOS	10
12	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – MONITORAMENTO E MITIGAÇÃO DE RISCOS ÀS IDENTIDADES DA TI	LICENÇA	200
13	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA SERVIDORES WINDOWS E LINUX/UNIX	LICENÇA	500
14	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA ESTAÇÕES	LICENÇA	2000
15	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – AUTENTICAÇÃO MULTI-FATOR COM INTELIGÊNCIA DE AMEAÇAS	LICENÇA	2000
16	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – GERENCIAMENTO DE CREDENCIAIS DAS IDENTIDADES DO USUÁRIO FINAL	LICENÇA	2000
17	PLATAFORMA DE REDE DE DISTRIBUIÇÃO DE CONTEÚDO - CDN	PACOTES DE 5 TERABYTES (TB)	8
18	SERVIÇOS ESPECIALIZADOS EM SEGURANÇA	UST	30.000

6.2. Especificação Detalhada:

6.2.1. A especificação detalhada dos itens 1 a 18 estão descritas no ANEXO B – CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS.

7. DA VIGÊNCIA DO CONTRATO

7.1. Os prazos de vigência e de execução contratual serão de 12 (doze) meses, podendo ser prorrogado, a critério da Contratante, com concordância da contratada, por períodos iguais ou inferiores, conforme art. 71 da Lei Federal 13.303/2016 e do art. 148 do Regulamento de Licitações e Contratos da ETICE.

7.2. Referido contrato poderá ser alterado nos casos previstos no art. 81 da Lei Federal n°13.303/2016 e no art. 149 do Regulamento de Licitações e Contratos da ETICE.

8. DO MODELO DE PROPOSTA

8.1. O modelo de proposta encontra-se no ANEXO D.

9. DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA

9.1. A gestão e fiscalização do contrato se darão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.

9.2. O Acordo de Níveis de Serviços está especificado no ANEXO A.

10. CONFIDENCIALIDADE DOS TRABALHOS

10.1. A Contratada, seu preposto e qualquer profissional da mesma, envolvidos na realização dos trabalhos, obrigam-se a tratar todas as informações obtidas junto a ETICE e seu clientefinal como **informação sigilosa ou confidencial**, devendo neste sentido mantê-las sob estrito sigilo, comprometendo-se ainda em não comunicar, divulgar ou revelar as informações confidenciais a terceiros, **mesmo após a finalização dos trabalhos a confidencialidade das informações permanecem**.

10.2. Para tal, serão consideradas como informações confidenciais todas e quaisquer informações ou dados, independentemente de estarem expressamente classificados como confidenciais, fornecidas verbalmente ou por escrito, ou de qualquer outra forma, corpórea ou não, cuja divulgação possa provocar prejuízos de qualquer natureza, abrangendo, mas não se limitando a, pormenores, estratégias de negócios, pesquisas, dados financeiros e estatísticos, informações sobre negociações em andamento, informações sobre softwares, informações cadastrais, documentos que venha a ter conhecimento ou acesso, ou que venha a receber da contratante, sejam de caráter técnico ou não.

10.3. Tais informações confidenciais deverão ser usadas exclusivamente para a condução dos trabalhos objeto da relação de serviços entre a ETICE, cliente final e a contratante, não podendo, sob nenhuma forma ou pretexto, serem divulgadas, reveladas, reproduzidas, utilizadas ou ser dado conhecimento a terceiros estranhos a esta contratação, exceto quando o dever de divulgar tais informações seja estritamente por força de exigência legal, devendo a parte obrigada a fornecer tais informações, avisar imediatamente a outra parte sobre tal exigência legal para, se for o caso, tomar as providências que achar necessárias.

10.4. A Contratada deverá apresentar "Termo de Responsabilidade e Sigilo", contendo a declaração de manutenção de sigilo e ciência das normas de segurança da Etice, assinado por cada empregado seu que estiverem diretamente envolvidos na contratação, quando o serviço exigir.

10.5. A contratada deverá entregar a ETICE, no momento da rescisão do contrato, todo o material físico ou digital de propriedade da contratante e destruir qualquer cópia em posse da contratada.

11. DA FRAUDE E DA CORRUPÇÃO

11.1. As Pré-Qualificadas devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

11.2. Para os propósitos deste item, definem-se as seguintes práticas:

11.2.1. "prática corrupta": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

11.2.2. "prática fraudulenta": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

11.2.3. "prática conluiada": esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

11.2.4. "prática coercitiva": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

11.2.5. "prática obstrutiva":

11.2.5.1 destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;

11.2.5.2 atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

11.3. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

11.4. Considerando os propósitos dos itens acima, a licitante vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

11.5. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

12. DA SUBCONTRATAÇÃO

12.1. Será admitida a subcontratação no limite de até 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016 e nos arts. 143 a 147 do Regulamento de Licitações e Contratos da ETICE, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

12.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a ETICE quanto à qualidade do objeto contratado, não constituindo, portanto, qualquer vínculo contratual ou legal da ETICE com a subcontratada.

12.3. A empresa subcontratada deverá atender, no que couber, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a licitante vencedora.

12.4. É vedada a subcontratação de empresa ou consórcio que tenha participado:

12.4.1. Do procedimento licitatório do qual se originou a contratação.

12.4.2. Direta ou indiretamente, da elaboração de projeto básico ou executivo.

13. DAS DISPOSIÇÕES GERAIS

13.1. **Esta chamada de oportunidade não importa necessariamente em contratação**, nos moldes já dispostos Edital de Pré-Qualificação 001/2019, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.

13.2. É facultada à Comissão de Avaliação ou à autoridade competente, em qualquer fase da licitação, **a promoção de diligência** destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação.

13.3. Toda a documentação fará parte dos autos e **não será devolvida a licitante**, ainda que se trate de originais.

13.4. Na contagem dos prazos estabelecidos nesta Chamada de Oportunidade, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. **Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente em dias úteis de expediente da ETICE.**

13.5. Os representantes legais das Pré-Qualificadas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

13.6. O desatendimento de exigências meramente formais, não essenciais, não implicará no afastamento da Pré-Qualificada, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

13.7. **A Comissão de Avaliação poderá sanar erros formais que NÃO acarretem prejuízos para o objeto da Chamada de Oportunidade**, a Administração e as Pré-Qualificadas, dentre estes, os decorrentes de operações aritméticas.

13.8. Desde já fica estabelecido que caso a Pré-Qualificada NÃO APRESENTE PROPOSTA para a presente Chamada de Oportunidade, já está renunciando, assim, expressamente ao direito de recurso e respectivas contrarrazões, concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem Nº 001/ 2019 – ETICE.

13.9. Os casos omissos serão resolvidos pela Comissão de Avaliação, nos termos da legislação pertinente.

13.10. As normas que disciplinam esta Chamada de Oportunidade serão sempre interpretadas em favor da ampliação da disputa.

13.11. Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, **possuem caráter sigiloso e serão disponibilizados exclusivamente aos órgãos de controle interno e externo**.

13.12. As Pré-Qualificadas deverão atender ao disposto no Código de Conduta, Ética e Integridade da ETICE, o qual encontra-se disponível no nosso sítio eletrônico para download.

13.13. O **foro** designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da **Comarca de Fortaleza**, Capital do Estado do Ceará.

Fortaleza,

Data: 07 de Agosto de 2023	**Data:** 07 de Agosto de 2023	**Data:** 08 de Agosto de 2023
Elaborado:	**De Acordo:**	**Aprovo:**
Francisco Augusto Andrade Maia *Analista de Gestão de TIC* *Diretoria de Tecnologia e Inovação (DITEC)*	**Márcio Adriano Castro Lima** *Diretor* *Diretoria de Tecnologia e Inovação (DITEC)*	**Francisco Antônio Martins Barbosa** *Presidente da Etice em Exercício*

ROL DE ANEXOS:

ANEXO A - GESTÃO DE NÍVEIS DE SERVIÇOS

ANEXO B - CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

ANEXO C - LISTA DE PERFIS TÉCNICOS

ANEXO D - CATÁLOGO DE SERVIÇOS

ANEXO E - MODELO DE PROPOSTA

ANEXO A - GESTÃO DE NÍVEIS DE SERVIÇOS

1.1. A gestão e fiscalização do contrato se darão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.

1.2. Será de responsabilidade da CONTRATANTE o atendimento de 1° nível.

1.3. Os chamados de 2° e 3° níveis fora dos horários acima e em dias úteis deverão ser atendidos pelo serviço de plantão, independentemente de ser sábado, domingo ou feriado. Os chamados de plantão incorrem em uma remuneração adicional medida em Unidades de Suporte Técnico (UST).

1.4. Os incidentes, situações inesperadas e não programadas, deverão ser atendidas pelos serviços de suporte da CONTRATADA. Os incidentes têm a seguinte classificação:

1.4.1. Severidade 1 ou Alta: Ambiente/Sistema está indisponível ou usuário sem acesso;

1.4.2. Severidade 2 ou Média: Uma função do Ambiente/Sistema está indisponível;

1.4.3. Severidade 3 ou Baixa: O Ambiente/Sistema está disponível, porém apresentando lentidão, erros que forçam o reinício do sistema e/ou de operações no mesmo, e/ou alguma intermitência em seu funcionamento.

1.5. A CONTRATADA deverá prestar, durante a vigência deste contrato, serviços de suporte a produção e manutenção corretiva abrangendo no mínimo:

1.6. Investigação e resolução de problemas no ambiente, mesmo que para isso seja necessário acionar o suporte do fabricante;

1.7. Nível de serviço (SLA), para chamados abertos entre o horário compreendido entre as 08 horas e 18 horas em dias úteis, conforme tabela a seguir:

Severidade	Natureza do Problema	Tempo de Resposta
Alta	Defeitos que tem como consequência a indisponibilidade do Ambiente / Sistema da CONTRATANTE	Até 10 (dez) horas contadas após registro do chamado, para diagnóstico e solução de contorno ou definitiva.
Média	Defeitos que tem como consequência a indisponibilidade parcial do Ambiente / Sistema da CONTRATANTE	Até 20 (vinte) horas úteis após registro do chamado, para diagnóstico e solução de contorno ou definitiva.
Baixa	Defeitos que não causam indisponibilidade do Ambiente / Sistema da CONTRATANTE, porém, impedem seu uso normal	Até 30 (trinta) horas úteis após registro do chamado, para diagnóstico e solução de contorno ou definitiva

1.8. Caso seja necessário complemento de informações para atendimento do chamado, que impossibilitem a resolução do chamado pela CONTRATADA, a CONTRATANTE será solicitada para fornecer a informação, e os prazos serão suspensos ou prorrogados até o recebimento das informações.

1.9. O tempo em horas, previsto no SLA, será computado a partir da abertura do chamado até a sua regularização, nesse caso, uma solução de contorno poderá ser utilizada, caso a solução definitiva não seja possível de ser executada imediatamente.

1.10. Em caso de atendimento presencial o SLA começa a ser contado a partir da chegada do técnico no local.

1.11. CONTRATADA deverá atender no mínimo 90% (noventa por cento) dos chamados dentro do SLA estabelecido na tabela.

ANEXO B - CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

1. CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

1.1. DETALHAMENTO DE ESPECIFICAÇÕES TÉCNICAS

1.1.1. ITEM 1 - SOLUÇÃO DE NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA OU PRIVADA.

1.1.1.1. CARACTERÍSTICAS GERAIS

1.1.1.1.1. PARA LICENCIAMENTO DE SOLUÇÃO DE NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA OU PRIVADA:

1.1.1.1.1.1. O licenciamento deverá ser feito pelo número de cores virtuais;

1.1.1.1.1.2. A solução deve estar listada como parceiro de segurança, pelo menos, da Amazon (AWS), Azure, Google Cloud Platform (GCP) e Oracle Cloud (OCI).

1.1.1.1.1.3. Deve ser compatível com, pelo menos, os seguintes hypervisors: VMware ESXi, Microsoft Hyper-V e KVM;

1.1.1.1.1.4. A solução deverá permitir expansão através de adição de novas licenças, de forma que supo. a criação de "pools" de gateways virtuais;

1.1.1.1.1.5. A solução para ambientes virtualizados deve suportar os seguintes SDN de mercado para integração, como: OpenStack, Cisco ACI, VMware NSX, e ESXi.

1.1.1.2. FUNCIONALIDADE DE FIREWALL

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

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

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

1.1.1.2.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

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

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

1.1.1.2.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, as identificando as regras mais utilizadas;

1.1.1.2.8. Deve suportar os seguintes tipos de NAT:

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

1.1.1.2.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.1.2.11. Deve suportar NAT64 e NAT46;

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

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

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

1.1.1.2.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.1.1.2.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.1.2.17. Suportar OSPF graceful restart;
1.1.1.2.18. Autenticação integrada via Kerberos.
1.1.1.2.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
1.1.1.2.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.1.3. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB PARA NUVEM PÚBLICA OU PRIVADA.

1.1.1.3.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;
1.1.1.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
1.1.1.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
1.1.1.3.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
1.1.1.3.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
1.1.1.3.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
1.1.1.3.6.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
1.1.1.3.6.2. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
1.1.1.3.6.3. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
1.1.1.3.7. A solução deve suportar a recategorização de URLs local;
1.1.1.3.8. Atualizar a base de assinaturas de aplicações automaticamente;
1.1.1.3.9. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
1.1.1.3.10. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
1.1.1.3.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
1.1.1.3.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
1.1.1.3.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
1.1.1.3.14. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
1.1.1.3.15. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
1.1.1.3.16. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
1.1.1.3.17. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
1.1.1.3.18. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;
1.1.1.3.19. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;
1.1.1.3.20. Suportar a criação de categorias de URLs customizadas;
1.1.1.3.21. Permitir a customização de página de bloqueio;

1.1.1.3.22. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do órgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou aplicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI;

1.1.1.3.23. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.1.3.24. 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);

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

1.1.1.3.25.1. PCI – números de cartão de crédito;
1.1.1.3.25.2. Arquivos PDF;
1.1.1.3.25.3. Arquivos executáveis;
1.1.1.3.25.4. Arquivos de banco de dados;
1.1.1.3.25.5. Arquivos do tipo documento;
1.1.1.3.25.6. Arquivos do tipo apresentação;
1.1.1.3.25.7. Arquivos do tipo planilha;

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

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

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

1.1.1.4.FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS PARA NUVEM PÚBLICA OU PRIVADA.

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

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

1.1.1.4.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.1.4.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

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

1.1.1.4.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.1.4.7. Detectar e bloquear a origem de portscans;

1.1.1.4.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.1.4.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.1.4.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.1.4.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.1.4.12. Suportar bloqueio de arquivos por tipo;

1.1.1.4.13. Identificar e bloquear comunicação com botnets;

1.1.1.4.14. Deve suportar referência cruzada com CVE;

1.1.1.4.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.1.4.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.1.4.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
1.1.1.4.18. Os eventos devem identificar o país de onde partiu a ameaça;
1.1.1.4.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
1.1.1.4.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
1.1.1.4.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
1.1.1.4.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
1.1.1.4.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.1.5.FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO PARA NUVEM PÚBLICA OU PRIVADA.

1.1.1.5.1. Suportar a criação de políticas de QoS por:
1.1.1.5.1.1. Endereço de origem, endereço de destino e por porta;
1.1.1.5.2. O QoS deve possibilitar a definição de classes por:
1.1.1.5.2.1. Banda garantida;
1.1.1.5.2.2. Banda máxima;
1.1.1.5.2.3. Fila de prioridade;

1.1.1.6.FUNCIONALIDADES DE VPN PARA NUVEM PÚBLICA OU PRIVADA.

1.1.1.6.1. Suportar VPN Site-to-Site e Cliente-To-Site;
1.1.1.6.2. Suportar IPSec VPN;
1.1.1.6.3. Suportar SSL VPN;
1.1.1.6.4. A VPN IPSEc deve suportar:
1.1.1.6.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;
1.1.1.6.5. A solução deve suportar CA Interna e CA Externa de terceiros;
1.1.1.6.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.1.7.SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS PARA NUVEM PÚBLICA OU PRIVADA.

1.1.1.7.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing;
1.1.1.7.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
1.1.1.7.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
1.1.1.7.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;
1.1.1.7.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;
1.1.1.7.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
1.1.1.7.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;
1.1.1.7.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.1.7.9. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.1.7.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.1.7.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.1.7.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;

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

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

1.1.1.7.14.1. Quantidade de arquivos que estão em emulação;

1.1.1.7.14.2. Número de arquivos emulados;

1.1.1.7.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.1.7.15.1. Arquivos scaneados;

1.1.1.7.15.2. Arquivos maliciosos;

1.1.1.8. GERENCIAMENTO CENTRALIZADO E RELATORIA PARA SOLUÇÃO DE NUVEM PÚBLICA OU NUVEM PRIVADA

1.1.1.8.1. Deve permitir o gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre;

1.1.1.8.2. O módulo de gerência deve ser capaz de gerenciar e administrar a solução descrita nesse item;

1.1.1.8.3. Caso a solução possua licenciamento por número de equipamentos gerenciados, deve ser entregue licenciada para a quantidade adquirida neste item;

1.1.1.8.4. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

1.1.1.8.5. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

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

1.1.1.8.7. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

1.1.1.8.8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

1.1.1.8.9. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

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

1.1.1.8.11. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.1.1.8.12. Suportar backup das configurações e rollback de configuração para a última configuração salva;

1.1.1.8.13. Suportar validação de regras antes da aplicação;

1.1.1.8.14. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

1.1.1.8.15. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

1.1.1.8.16. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

1.1.1.8.17. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.1.1.8.18. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;
1.1.1.8.19. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;
1.1.1.8.20. Deve ser possível exportar os logs em CSV;
1.1.1.8.21. Deve possibilitar a geração de relatórios de eventos no formato PDF;
1.1.1.8.22. Possibilitar rotação do log;
1.1.1.8.23. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
1.1.1.8.24. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;
1.1.1.8.25. Deve permitir a criação de relatórios personalizados;
1.1.1.8.26. Suportar enviar os relatórios de forma automática via PDF:
1.1.1.8.27. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.
1.1.1.8.28. Deve consolidar logs e relatórios de todos os dispositivos administrados;
1.1.1.8.29. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
1.1.1.8.30. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
1.1.1.8.31. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
1.1.1.8.32. Permitir que os relatórios possam ser salvos, enviados e impressos;
1.1.1.8.33. Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;
1.1.1.8.34. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc.;
1.1.1.8.35. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
1.1.1.8.36. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
1.1.1.8.37. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
1.1.1.8.38. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
1.1.1.8.39. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
1.1.1.8.40. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
1.1.1.8.41. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;
1.1.1.8.42. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;
1.1.1.8.43. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;
1.1.1.8.44. Permitir a visualização de gráficos e mapa de ameaças;
1.1.1.8.45. Possuir mecanismo para que logs antigos sejam removidos automaticamente;
1.1.1.8.46. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
1.1.1.8.47. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
1.1.1.8.48. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;
1.1.1.8.49. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;
1.1.1.8.50. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

1.1.2.ITEM 2 - SOLUÇÃO DE AUTOMAÇÃO DE GOVERNANÇA, POSTURA E CONFORMIDADE PARA NUVENS PÚBLICAS

1.1.2.1.REQUISITOS DE USABILIDADE

1.1.2.1.1. A solução deve ser SaaS, sem a necessidade de instalação de agentes, servidores ou containers adicionais;

1.1.2.1.2. Deve ser possível escalar a adoção da solução de maneira simples e rápida;

1.1.2.1.3. A solução deve funcionar por meio de chamadas API, permitindo uma integração simples;

1.1.2.1.4. A solução deve suportar os principais servidores de nuvem, como (mas não se limitando à) AWS, Azure, GCP;

1.1.2.1.5. A solução deve consistir em uma plataforma única com CSPM, CWPP, e Threat Inteligence permitindo ao administrador ter uma mesma experiência para o ambiente multi-cloud;

1.1.2.1.6. A solução deve prover uma visualização geral dos ativos protegidos e problemas mais urgentes, porém com a possibilidade de customização de acordo com o que o administrador julgar melhor;

1.1.2.1.7. A solução deve possuir suporte à grandes empresas, MSSP e Service Providers;

1.1.2.1.8. A solução deve possuir cobertura abrangente para os diversos serviços oferecidos por cada um dos provedores de nuvem;

1.1.2.1.9. A solução deve funcionar como um painel central para gestão das diferentes clouds;

1.1.2.1.10. A solução deve garantir diretrizes de segurança aos clusters de Kubernetes;

1.1.2.1.11. A solução deve possuir cobertura à diversos tipos de entidades e serviços em diferentes cenários, como AWS, Azure, GCP, Kubernetes, e Terraform;

1.1.2.2.REQUISITOS DE VISIBILIDADE

1.1.2.2.1. A solução deve permitir com que cada um de seus usuários realize customizações nos painéis de visualização como julgarem melhor, que por sua vez, devem escolher entre compartilhar ou não essa nova visualização com os demais administradores da solução;

1.1.2.2.2. A solução deve entregar resultados de compliance em no máximo 5 minutos e alertas relacionados à eventos identificados em até 30 minutos, sendo desconsideradas soluções que demorem mais de 1 hora para exibir dados sobre um novo ativo ou alertas de segurança;

1.1.2.2.3. A solução deve gerar, de maneira automatizada, uma topologia do ambiente, interrelacionando os security groups de acordo com as permissões existentes neles;

1.1.2.2.4. A solução deve possuir visibilidade de assets e grupos de segurança plotada em tempo real, incluindo novas modificações realizadas nas VPCs/vNets quanto nos grupos de segurança;

1.1.2.2.5. A solução deve permitir uma visualização da postura de segurança de rede para configurações incorretas em grupos de segurança;

1.1.2.2.6. A solução deve permitir uma visualização da postura de segurança de rede para visualização de VPCs/vNets;

1.1.2.2.7. Deve ser possível observar quais redes privadas em nuvem (VPCs & vNets) possuem comunicação entre redes;

1.1.2.2.8. A solução deve permitir que os administradores tenham uma visualização do fluxo de tráfego e de tráfego bloqueado entre ativos de nuvem - grupos de segurança, instâncias, etc.

1.1.2.2.9. A solução deve ser capaz de realizar um inventário de todos os ativos protegidos, políticas de segurança e política de segurança efetiva para os ativos de nuvem;

1.1.2.2.10. A solução deve ter recursos integrados de geração de relatórios sobre eventos/descobertas de segurança;

1.1.2.2.11. A solução deve ser capaz de avaliar a postura com base nas configurações nativas da nuvem, bem como nas descobertas de terceiros;

1.1.2.2.12. A solução deve auditar as alterações na solução ou nas contas de nuvem conectadas à ela;

1.1.2.2.13. A solução deve gerenciar e controlar centralmente a autenticação e autorização do usuário;

1.1.2.2.14. A solução deve apresentar os resultados das avaliações de forma legível por humanos e por máquina, por meio de relatórios e integrações com soluções terceiras;

1.1.2.2.15. A solução deve, além de encontrar portas abertas em ativos críticos, remediar eventos, gerar relatórios globais para garantir conformidade e melhores práticas de segurança;

1.1.2.2.16. A solução deve detectar configurações incorretas para qualquer ambiente de nuvem que tenha sido vinculado à solução;

1.1.2.2.17. A solução deve fornecer uma revisão de arquitetura de segurança de alto nível do ambiente em nuvem, identificando possíveis riscos de segurança, além de inspecionar e visualizar exposições de políticas de rede;

1.1.2.2.18. A solução deve fornecer diagramas de rede atualizados (SecOps);

1.1.2.2.19. A solução deve validar se há algum envio/recebimento de tráfego de rede não autorizado e que o tráfego de segurança de rede em todos os provedores de nuvem está sendo monitorado em tempo real, com o intuito de garantir as melhores práticas;

1.1.2.2.20. Deve ser possível correlacionar logs identificados à técnicas e táticas presentes no framework do MITRE ATT&CK;

1.1.2.3. REQUISITOS DE VISIBILIDADE DE REGULAMENTAÇÕES

1.1.2.3.1. A solução deve fornecer cobertura de verificação de aderência à diversas regulamentações para, pelo menos, AWS, Azure, GCP e Kubernetes;

1.1.2.3.2. A solução deve fornecer cobertura à, pelo menos, 40 regulamentações relacionadas aos diferentes tipos de ambiente em nuvem;

1.1.2.3.3. A solução deve ser capaz de medir riscos de soluções IaaS e PaaS, bem como aderência à regulamentações distintas;

1.1.2.3.4. A solução deve possuir pelo menos 1000 verificações de compliance por padrão, a partir do momento em que um novo tenant é criado;

1.1.2.3.5. A solução deve permitir a customização das regras de validação de compliance, sendo realizada de maneira simples, sem a necessidade de aprender uma linguagem de programação para isso;

1.1.2.3.6. A solução deve permitir uma fácil personalização de verificações de segurança com base em requisitos de governança definidos por regulamentações, como ISO27001 e GDPR;

1.1.2.3.7. A solução deve fornecer suporte contínuo ao processo de conformidade com personalizações que permitem relatórios e integração fáceis e significativos em processos contínuos de conformidade e operações de nuvem;

1.1.2.3.8. A solução deve fornecer recursos de avaliação para ambos os recursos implantados, bem como implantações prospectivas, conforme definido pelos modelos de IaC (Terraform, CFTs);

1.1.2.3.9. A solução deve permitir que diferentes contas e/ou regiões estejam sujeitas a diferentes políticas de avaliação;

1.1.2.3.10. A solução deve permitir avaliações contínuas do nível de postura;

1.1.2.3.11. A solução deve permitir que os usuários criem regras e conjuntos de regras personalizados para avaliar a postura sem escrever código;

1.1.2.3.12. A solução deve executar relatórios globais para garantir conformidade, melhores práticas de segurança e encontrar portas abertas em ativos críticos e remediar;

1.1.2.3.13. A solução deve garantir que os recursos de nuvem que lidam com dados em repouso (S3/BLOB, EBS, RDS, VMs, etc.), sejam marcados e criptografados adequadamente;

1.1.2.3.14. A solução deve ser capaz de analisar e garantir que todos os componentes de uma implantação estejam usando criptografia TLS ao se comunicar com outras camadas;

1.1.2.3.15. A solução deve ser capaz de avaliar a postura em relação às principais estruturas/melhores práticas de conformidade do setor prontas para uso;

1.1.2.3.16. A solução deve gerar um relatório de conformidade em todas as contas de nuvem que precisem passar por uma validação de um padrão de conformidade;

1.1.2.4. REQUISITOS DE CONTROLE

1.1.2.4.1. A solução deve ser baseada em API e nela deve ser possível realizar controles e correções sobre o ambiente em nuvem;

1.1.2.4.2. A solução deve permitir uma correção automática de violações de conformidade e governança e realizar correção automática sem permissões de escrita no ambiente em nuvem, utilizando CloudBots;
1.1.2.4.3. A solução deve proteger os ambientes de nuvem contra edição não autorizada para evitar desvios de configuração de segurança;
1.1.2.4.4. A solução deve realizar monitoramento de usuários privilegiados, detectar anomalias, comprometimento de contas e chaves de acesso e casos de uso avançados de UEBA (Comportamento Analítico de Usuários e Entidades);
1.1.2.4.5. A solução deve corrigir automaticamente configurações incorretas e problemas encontrados, sem intervenção humana e sem acesso de gravação sensível ao ambiente;
1.1.2.4.6. A solução deve ser capaz de aplicar a política de autenticação da empresa;
1.1.2.4.7. A solução deve ser capaz de aplicar a política de segurança de rede da empresa;
1.1.2.4.8. A solução deve proteger os ambientes de nuvem contra alterações não autorizadas em vários provedores de nuvem;
1.1.2.4.9. A solução deve ser capaz de impedir que alterações de rede sejam feitas em grupos de segurança;
1.1.2.4.10. A solução deve fornecer acesso remoto "just in time" para porta/protocolo e destino IP, no caso de uma manutenção precisar ser executada por uma equipe terceira ou colaboradores que não têm acesso liberado à determinado recurso;
1.1.2.4.11. A solução deve garantir que os usuários, grupos e funções do IAM da AWS não contenham privilégios excessivamente permissivos, especialmente em funções de instância;
1.1.2.4.12. A solução deve ser capaz de limitar o tempo de acesso à console da AWS acessos permissivos;

1.1.2.5. REQUISITOS DE INTEGRAÇÕES

1.1.2.5.1. A solução deve possuir suporte à integração com ferramentas nativas (Inspector, Guard Duty etc.);
1.1.2.5.2. A solução deve suportar alertas de avaliação a serem encaminhados por, pelo menos, e-mail. Slack, AWS SNS, Service Now e ferramenta de SOC do próprio provedor de nuvem;
1.1.2.5.3. A solução deve fornecer APIs RESTless permitindo acesso via API para criação/visualização de regras e conjuntos de regras, para criação de políticas de conformidade contínua e para consumo dos resultados de avaliações anteriores;
1.1.2.5.4. A solução deve permitir conexão de maneira simples ao pipeline de CI/CD;

1.1.3. ITEM 3 - SOLUÇÃO DE PROTEÇÃO PARA APLICAÇÕES WEB EM NUVEM (WAF), DEFESA DE API E AUTOMAÇÕES (BOTS)

1.1.3.1. Suportar as seguintes tecnologias de proteção:
1.1.3.1.1. Web Application Protection
1.1.3.1.2. API Security
1.1.3.1.3. Bot Prevention
1.1.3.1.4. Intrusion Prevention (IPS)
1.1.3.2. A solução deve permitir uma quantidade ilimitada de aplicações ou largura de banda, uma vez que a solução fornecerá proteção a diferentes ambientes WEB e API e o número dessas aplicações é muito dinâmico, bem como a quantidade de largura de banda e sua localização (nuvem/on-premise).
1.1.3.3. A solução deve ser licenciada por número de requisições WEB conforme tabela de quantitativos. As quantidades contratadas poderão ser utilizadas por até 12 meses.
1.1.3.4. A solução deve ser capaz de evitar ataques cibernéticos conhecidos e desconhecidos.
1.1.3.5. A implementação deve ser flexível e pode ser realizada em diferentes ambientes na nuvem e on-premises.
1.1.3.6. A solução deve ser gerenciada a partir de um portal em nuvem.
1.1.3.7. A solução deve ser capaz de proteger aplicações em diferentes ambientes e em qualquer arquitetura (on-premise, cloud, containers) gerenciada a partir de um único portal centralizado.
1.1.3.8. A solução deve ser capaz de analisar cada solicitação recebida, e esta solicitação deve ser analisada em contexto.
1.1.3.9. A solução deve ser capaz de realizar análise de risco, examinando parâmetros como:
1.1.3.9.1. Perfil do usuário;

1.1.3.9.2. Padrões observados na sessão do usuário;
1.1.3.9.3. A forma como outros usuários normalmente interage com a aplicação;
1.1.3.10. A solução deve ser capaz de bloquear os seguintes tipos de ataques:
1.1.3.10.1. Cross Site Request Forgery;
1.1.3.10.2. XML External Entity;
1.1.3.10.3. Remote Code Execution;
1.1.3.10.4. Evasion Techniques;
1.1.3.10.5. LDAP Injection;
1.1.3.10.6. Path Traversal;
1.1.3.10.7. Vulnerability Scanning;
1.1.3.10.8. SQL Injection;
1.1.3.10.9. Métodos HTTP ilegais;
1.1.3.10.10. Entrada inválida para formulários;
1.1.3.10.11. Scraping Brute Force Attacks;
1.1.3.10.12. Pelo menos 2800 CVEs específicos da Web;
1.1.3.11. A solução deve ser capaz de configurar exceções como:
1.1.3.11.1. Uma expressão regular que determina o URI que deve coincidir. Por exemplo: /login/*.
1.1.3.11.2. Expressão regular e CIDR que determina o identificador de origem que deve corresponder. Por exemplo 192.168.24.0/24 ou. * @ xxxx.com)
1.1.3.11.3. Um CIDR que determina o IP de origem física que deve coincidir. Por exemplo: 192.168.24.0/16
1.1.3.11.4. Uma expressão regular que determina o nome do parâmetro que deve coincidir. Por exemplo: * Senha *
1.1.3.11.5. Uma expressão regular que determina o nome do parâmetro que deve coincidir. Por exemplo: ^ 4 [0-9] {12} (?: [0-9] {3})? $)
1.1.3.11.6. Um indicador que deve coincidir. Se necessário, usar uma lista separada por vírgulas.
1.1.3.11.7. A solução deve ser capaz de configurar exceções e modificar as ações tomadas pela ferramenta por padrão, e deve permitir a aceitação ou bloqueio do tráfego quando corresponder a algumas das condições mencionadas.
1.1.3.11.8. A solução deve permitir upload de certificados para proteger sites HTTPS da instituição.
1.1.3.11.9. A solução precisará incluir um mecanismo de aprendizagem que ajude a diminuir o número de eventos críticos e altos ao longo do tempo à medida que aprende o tráfego do site e entende o comportamento do usuário.
1.1.3.11.10. O aprendizado da solução deve funcionar continuamente e não apenas ter um "modo de aprendizagem".
1.1.3.11.11. A solução precisará classificar cada solicitação e decidir suas possibilidades de ataque através de um mecanismo inteligente de inteligência artificial.
1.1.3.11.12. As políticas de solução devem ser capazes de operar em pelo menos os seguintes modos:
1.1.3.11.13. Prevenção
1.1.3.11.14. Aprendizado/Detecção
1.1.3.11.15. Desabilitado
1.1.3.11.16. A solução deve incluir políticas predefinidas que sejam práticas recomendadas (ou a prática recomendada pelo fabricante). Essas políticas devem ser editáveis, se necessário.
1.1.3.11.17. A solução deve ser capaz de ser instalada em diferentes ambientes, alguns atualmente implementados na instituição e outros que serão implementados no futuro, pelo menos ela deve ser capaz de ser instalado em:
1.1.3.11.17.1. Cloud: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, VMware
1.1.3.11.17.2. Contêineres: Docker, Kubernetes, Kubernetes Ingress, Openshift
1.1.3.11.17.3. Um agente que funciona em NGINX Web Server ou em um proxy reverso NGINX
1.1.3.11.18. A solução deve permitir que você aplique políticas para definir limites em mensagens de protocolo HTTP. Inclua pelo menos os seguintes parâmetros:
1.1.3.11.18.1. Tamanho do corpo — tamanho máximo do corpo da mensagem HTTP
1.1.3.11.18.2. Tamanho do URL — Tamanho máximo de URL, isso inclui todos os campos de consulta.
1.1.3.11.18.3. Tamanho do cabeçalho (Header Size): tamanho máximo do cabeçalho HTTP

1.1.3.11.18.4. Profundidade máxima do objeto: Tamanho máximo de profundidade do objeto JSON/XML, isso inclui XML incorporado no JSON e o oposto.

1.1.3.11.18.5. Métodos de HTTP Válidos (RFP): Aceitar ou bloquear métodos http não padrão

1.1.3.11.19. A solução deve suportar métodos para ser capaz de distinguir os usuários uns dos outros. Ele deve suportar pelo menos os seguintes mecanismos:

1.1.3.11.19.1. X-Forwarded-For

1.1.3.11.19.2. IP Origem

1.1.3.11.19.3. Cookie

1.1.3.11.19.4. Header Only

1.1.3.11.20. A solução deve fornecer proteção proativa para potenciais vulnerabilidades de API através de um procedimento de validação de esquema

1.1.3.11.21. A solução deve rever as solicitações de API recebidas com esses esquemas para bloquear todas as solicitações inválidas.

1.1.3.11.22. A solução deve ser capaz de proteger APIs usando técnicas como validação automatizada usando arquivos de esquema OpenAPI.

1.1.3.11.23. A solução precisará ser capaz de injetar scripts em páginas de aplicações Web, como páginas de login, ou usar algum outro mecanismo para coletar dados sobre padrões de entrada e sequências de digitação, movimentos do mouse. Isso para ser capaz de diferenciar um humano de um bot.

1.1.3.11.24. A solução deve ser capaz de identificar esses padrões no caso de um bot usá-los.

1.1.3.11.25. A solução deve ser capaz de tomar uma decisão se a entrada é inserida por um humano ou por um script automático (como um bot) e bloquear essa atividade.

1.1.3.11.26. O recurso IPS precisará fornecer proteções tradicionais baseadas em assinaturas para pelo menos 2800 CVEs baseados na Web (vulnerabilidades e exposições comuns).

1.1.3.11.27. A solução de gerência deve ser baseada em nuvem ou através de appliance dedicado do próprio fabricante, não sendo soluções baseada em servidores abertos;

1.1.3.11.28. A gerência deve possuir visibilidade de todos os eventos de segurança e auditoria;

1.1.3.11.29. Deve gerenciar e administrar de forma centralizada, todas as soluções de proteção para aplicação do mesmo fabricante desde que não sejam software livre;

1.1.3.11.30. O licenciamento para armazenamento da solução deve suportar escalabilidade no volume de logs.

1.1.3.11.31. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pela solução de segurança;

1.1.3.11.32. Centralizar a administração de regras e políticas da solução de segurança, usando uma única interface de gerenciamento;

1.1.3.11.33. Deve permitir a visualização dos logs de uma regra específica na mesma tela de configuração da regra selecionada;

1.1.3.11.34. Suportar geração de logs de auditoria, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.1.3.11.35. A solução de gerência deve apresentar eventos em um unico portal (dashboard), de todas as funcionalidades de segurança que estão ativadas. Sendo que deve possuir telas de apresentação onde consta todo os principais eventos de forma consolidada como: atividades maliciosas, linha do tempo dos principais incidentes, estatisticas das applicações protegidas (assets), severidade dos ataques;

1.1.3.11.36. A solução deve permitir o login de multiplos usuários administradores simultaneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.1.3.11.37. Deve permitir a criação de filtros nos eventos encontrados, tais como a severidade do evento, nome da aplicação protegida, ação, tipo do ataque, origem, método HTTP, HTTP host e HTTP URI path;

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

1.1.3.11.38.1. Visualizar quantidade de tráfego realizados nas aplicações;

1.1.3.11.38.2. Gráficos com principais eventos de segurança;

1.1.3.11.39. A solução deve notificar o administrador classificando a severidade do evento;

1.1.3.11.40. A notificação deve conter informações de forma clara, para que permita o administrador tomar uma ação para remediar o incidente ocorrido;

1.1.4.ITEM 4 - SOLUÇÃO PARA ANÁLISE DE SEGURANÇA EM DESENVOLVIMENTO DE CÓDIGO FONTE

1.1.4.1. CARACTERÍSTICAS GERAIS

1.1.4.1.1. A console de administração deve ser SaaS (Software as a Service), hospedada na nuvem do fabricante, sem a necessidade de instalação de agentes, servidores ou containers adicionais na infraestrutura do cliente

1.1.4.1.2. Deve ser possível escalar a adoção da solução de maneira simples e rápida

1.1.4.1.3. A solução deve permitir integração via APIs

1.1.4.1.4. A solução deve classificar os tipos de repositórios ou esteiras de desenvolvimento de maneira automática na plataforma, ex: realizado a integração com GitHub, a ferramenta deve mostrar na console de forma correta a fonte integrada

1.1.4.1.5. A solução deve prover uma visualização geral dos ativos/repositórios protegidos e problemas mais urgentes

1.1.4.1.6. A solução deve possuir cobertura abrangente e integração nativa com diversas ferramentas de CI-CD e repositórios de código

1.1.4.1.7. A solução deve funcionar como um painel central para gestão dos diferentes repositórios/projetos

1.1.4.1.8. A ferramenta devera possuir mecanismo RBAC (Role based access control)

1.1.4.1.9. A ferramenta deverá estar licenciada para a quantidade de desenvolvedores especificados na tabela de quantitativos;

1.1.4.2. REQUISITOS DE INTEGRAÇÕES E CAPACIDADES

1.1.4.2.1. A solução de análise de código deve executar um mecanismo de correspondência hierárquica, o que significa que contém uma expressão padrão, e cada padrão pode conter outra expressão padrão, a qual cada padrão pode conter várias outras expressões padrões e assim por diante.

1.1.4.2.2. Cada padrão pode ter uma variedade de testadores. De forma que pequenos detectores criados especificamente para os tipos de dados, possam se misturar e combinar. Desta forma, criando um mecanismo de consulta robusto e um analisador estático para procurar falhas nos padrões de segurança.

1.1.4.2.3. A ferramenta deve ser agnóstica ao código, ou seja, deve analisar qualquer tipo de linguagem de programação

1.1.4.2.4. A ferramenta deve realizar o scan e buscar no mínimo os seguintes riscos de segurança dentro do código, repositórios de código, IaCs (Infraestrutura como código) e binários:

1.1.4.2.4.1. Senhas
1.1.4.2.4.2. Tokens
1.1.4.2.4.3. API keys
1.1.4.2.4.4. Credenciais
1.1.4.2.4.5. OWASP:
1.1.4.2.4.6. A2:2017 - Broken Authentication
1.1.4.2.4.7. A3:2017 - Sensitive Data Exposure
1.1.4.2.4.8. A5:2017 - Broken Access Control
1.1.4.2.4.9. A6:2017 - Security Misconfiguration
1.1.4.2.4.10. Falhas ou má configuração em IaCs, baseado nos padrões pré-definidos da ferramenta
1.1.4.2.4.11. Deve possibilitar a criação de padrões próprios de detectores a fim de customizar o scan da ferramenta

1.1.4.2.5. A ferramenta deve ser capaz de detectar padrões não adequados ao framework PCI

1.1.4.2.6. A ferramenta de forma nativa devera prover ao menos 1000 tipos de detectores, a fim de automatizar as detecções com os padrões da ferramenta

1.1.4.2.7. A solução deve prover diversos métodos de scan:

1.1.4.2.7.1. Realizar o scan de código em busca das informações que estejam "hard-coded" em todo o SDLC (Software development life cycle), em seu SCM (software/Ferramenta de sypply chain), estareiras de CI-CD ou diretamente no computador que esta sendo executado

1.1.4.2.7.2. Scan de IaC (Infrastructure as a Code) – realizar o scan em arquivos Terraform, Helm e Kubernets em busca de problemas ou falhas de configuração que possam introduzir risco a aplicação

1.1.4.2.8. A ferramenta não deve armazenar o código fonte analisado na plataforma em nuvem, ou seja, deve manter somente os metadados com as informações relevantes do que foi encontrado.

1.1.4.2.9. Em caso de encontrar alguma senha exposta ou erro de configuração, por exemplo, a ferramenta devera:

1.1.4.2.9.1. Mostrar o mecanismo de detecção utilizado

1.1.4.2.9.2. O caminho onde foi encontrado, ou seja, o path e a linha de código

1.1.4.2.9.2.1. Clicando sobre o erro, deve direcionar para a linha de código onde o mesmo se encontra, ou arquivo de configuração ou pipeline

1.1.4.2.9.3. Prover uma descrição clara do problema encontrado

1.1.4.2.9.4. Prover uma recomendação para correção/remediação

1.1.4.2.10. A Ferramenta deve prover integração nativa com pelo menos os seguintes repositórios de código:

1.1.4.2.10.1. GitLab

1.1.4.2.10.2. GitHub

1.1.4.2.10.3. Repositórios locais

1.1.4.2.11. A Ferramenta deve prover integração nativa com pelo menos as seguintes ferramentas de CI-CD (pipeline):

1.1.4.2.11.1. GitLab Ci-CD

1.1.4.2.11.2. GitHub Action

1.1.4.2.11.3. Jenkins

1.1.4.2.11.4. Azure DevOps

1.1.4.2.11.5. BitBucket pipeline

1.1.4.2.12. A Ferramenta deve prover integração com ferramentas de colaboração para análise dos códig compartilhados nas mesmas, deve possuir integração com pelo menos:

1.1.4.2.12.1. Confluence

1.1.4.2.12.2. Slack

1.1.4.2.12.3. Teams

1.1.4.2.13. A ferramenta deve prover integração com ferramenta de tarefas/chamados, como Jira, assim, em caso de encontrar alguma violação de segurança, deverá abrir um ticket automaticamente na ferramenta de chamados.

1.1.4.2.13.1. Deve possuir suporte a SSO via SAML 2.0

1.1.4.2.13.2. Deve possibilitar exportar os resultados das detecções nos formatos JSON e CSV

1.1.4.2.13.3. Deve possuir uma visão gráfica dos problemas encontrados

1.1.4.2.13.4. Deve possuir relatórios que possam ser exportados em pelo menos formato PDF

1.1.5. ITEM 5 - SOLUÇÃO DE ANÁLISE E GESTÃO INTELIGENTE DE VULNERABILIDADE PARA RECURSOS DE NUVEM

1.1.5.1. CARACTERÍSTICAS GERAIS

1.1.5.1.1. A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuraçã conformidade (baseline e compliance);

1.1.5.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

1.1.5.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

1.1.5.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

1.1.5.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

1.1.5.1.5.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

1.1.5.1.6. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

1.1.5.1.7. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;

1.1.5.1.8. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

1.1.5.1.9. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

1.1.5.1.9.1. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

1.1.5.1.10. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

1.1.5.1.11. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

1.1.5.1.12. O escaneamento para os dispositivos expostos deve sem realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;

1.1.5.1.13. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;

1.1.5.1.14. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

1.1.5.1.15. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

1.1.5.1.16. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

1.1.5.1.17. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

1.1.5.1.18. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

1.1.5.1.19. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

1.1.5.1.20. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

1.1.5.1.21. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

1.1.5.1.22. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

1.1.5.1.23. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

1.1.5.1.24. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

1.1.5.1.25. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;

1.1.5.1.26. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

1.1.5.1.27. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

1.1.5.2. DOS REQUISITOS E RELATÓRIOS E PAINÉIS GERENCIAIS

1.1.5.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

1.1.5.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;

1.1.5.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

1.1.5.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;

1.1.5.2.5. A solução deve permitir a customização de dashboards/relatórios;

1.1.5.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

1.1.5.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;

1.1.5.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

1.1.5.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

1.1.5.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;

1.1.5.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

1.1.5.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

1.1.5.3. DAS VARREDURAS

1.1.5.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

1.1.5.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

1.1.5.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

1.1.5.3.3.1. Tais agentes devem realizar conexões para o sistema gerenciamento através de protoc seguro;

1.1.5.3.4. A solução deve ser configurável para permitir a otimização das configurações de varredura;

1.1.5.3.5. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

1.1.5.3.6. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

1.1.5.3.7. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

1.1.5.3.7.1. CyberArk;

1.1.5.3.7.2. BeyondTrust;

1.1.5.3.7.3. Thycotic;

1.1.5.3.7.4. Centrify;

1.1.5.3.8. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

1.1.5.3.9. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

1.1.5.3.10. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

1.1.5.3.11. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades n seguintes tecnologias:

1.1.5.3.11.1. Cloud Services;

1.1.5.3.11.2. Data Leakage;

1.1.5.3.11.3. Database;

1.1.5.3.11.4. IoT;

1.1.5.3.11.5. Mobile Devices;

1.1.5.3.11.6. Operating System;

1.1.5.3.11.7. Peer-To-Peer;

1.1.5.3.11.8. SCADA;

1.1.5.3.11.9. Web Servers;

1.1.5.3.11.10. Web Clients;

1.1.5.3.12. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

1.1.5.3.13. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

1.1.5.4. DA ANÁLISE E PRIORIZAÇÃO DE VULNERABILIDADES

1.1.5.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

1.1.5.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

1.1.5.4.2.1. CVSS Impact Score;

1.1.5.4.2.2. Idade da Vulnerabilidade;

1.1.5.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;

1.1.5.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

1.1.5.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;

1.1.5.4.2.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

1.1.5.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

1.1.5.4.3. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

1.1.5.5. DA ANÁLISE DE RISCO DO AMBIENTE

1.1.5.5.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

1.1.5.5.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

1.1.5.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

1.1.5.5.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

1.1.5.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

1.1.5.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

1.1.5.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

1.1.5.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

1.1.5.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

1.1.5.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

1.1.5.5.11. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;

1.1.5.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

1.1.5.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

1.1.5.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

1.1.5.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

1.1.5.6. DA DESCOBERTA DE ATIVOS

1.1.5.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

1.1.5.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

1.1.5.6.2.1. Enumeração de Hosts;
1.1.5.6.2.2. Identificação de Sistema Operacional (SO);
1.1.5.6.2.3. Port Scan (Portas comuns);
1.1.5.6.2.4. Port Scan (Todas as portas);
1.1.5.6.2.5. Customizado;

1.1.5.6.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

1.1.5.6.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

1.1.5.6.4.1. Descoberta de Host;
1.1.5.6.4.2. Ping o host remoto;
1.1.5.6.4.3. Usar descoberta rápida;
1.1.5.6.4.4. Métodos de ping;
1.1.5.6.4.4.1. ARP;
1.1.5.6.4.4.2. TCP;
1.1.5.6.4.4.3. ICMP;
1.1.5.6.4.4.4. UDP;
1.1.5.6.4.5. Escaneamento de descoberta de dispositivos de OT/SCADA;
1.1.5.6.4.6. Escaneamento de descoberta em redes de impressora;
1.1.5.6.4.7. Escaneamento em redes Novell;
1.1.5.6.4.8. Tecnologia de Wake-on-LAN;

1.1.5.6.5. Port Scanning:

1.1.5.6.5.1. Portas;
1.1.5.6.5.1.1. Considerar portas não escaneadas como fechadas;
1.1.5.6.5.1.2. Range de portas a serem escaneadas;
1.1.5.6.5.2. Enumerar Portas locais:
1.1.5.6.5.2.1. SSH (netstat);
1.1.5.6.5.2.2. WMI (netstat);
1.1.5.6.5.2.3. SNMP;

1.1.5.6.6. Descoberta de Serviços:

1.1.5.6.6.1. Sondar todas as portas para encontrar serviços;
1.1.5.6.6.2. Procurar por serviços baseado em SSL/TLS;
1.1.5.6.6.3. Enumerar todas as cifras SSL/TLS;

1.1.5.6.7. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

1.1.5.6.8. A solução deve descobrir passivamente quando um host é adicionado na rede;

1.1.5.7. DA AVALIAÇÃO DE VULNERABILIDADE

1.1.5.7.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

1.1.5.7.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

1.1.5.7.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

1.1.5.7.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

1.1.5.7.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

1.1.5.7.6. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação:

1.1.5.7.6.1. Contas administrativas vulneráveis a Kerberoasting attack;
1.1.5.7.6.2. Utilização de criptografia vulnerável com autenticação Kerberos;
1.1.5.7.6.3. Contas com pré-autenticação do Kerberos desabilitada;

1.1.5.7.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
1.1.5.7.6.5. Verificar validação de fragilidades do tipo "Unconstrained Delegation";
1.1.5.7.6.6. Verificação de "Pre-Windows 2000 Compatible Access";
1.1.5.7.6.7. Verificação de validade de chaves mestras "Kerberos KRBTGT";
1.1.5.7.6.8. Verificação de "SID History Injection";
1.1.5.7.6.9. Verificação de "Printer Bug Exploit";
1.1.5.7.6.10. Verificação de "Primary Group ID";
1.1.5.7.6.11. Verificação de usuários com Passwords em branco;
1.1.5.7.6.12. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

1.1.5.7.7. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

1.1.5.7.8. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

1.1.5.7.9. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;

1.1.5.7.10. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

1.1.5.7.11. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

1.1.5.7.12. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;

1.1.5.7.13. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;

1.1.5.7.14. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;

1.1.5.7.15. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

1.1.5.7.16. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

1.1.5.7.17. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

1.1.5.7.18. A solução deve possuir importação de arquivos .YARA;

1.1.5.7.19. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

1.1.5.8. DA AUDITORIA DE CONFIGURAÇÃO

1.1.5.8.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

1.1.5.8.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

1.1.5.8.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

1.1.5.8.3.1. Center for Internet Security Benchmarks (CIS);
1.1.5.8.3.2. Defense Information Systems Agency (DISA) STIGs;
1.1.5.8.3.3. Health Insurance Portability and Accountability Act (HIPAA);
1.1.5.8.3.4. Payment Card Industry Data Security Standards (PCI DSS);

1.1.5.8.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

1.1.5.8.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

1.1.5.8.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

1.1.5.8.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

1.1.6.ITEM 6 - SOLUÇÃO PARA INSPEÇÃO DE TRÁFEGO E ACESSO SEGURO À INTERNET

1.1.6.1. CARACTERÍSTICAS GERAIS

1.1.6.1.1. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço, utilizando um único agente instalado na máquina do usuário ou através de composição de soluções.

1.1.6.1.2. A nuvem do fabricante deverá ser distribuída globalmente em pelo menos 30 pontos de presença globais, incluindo o Brasil.

1.1.6.1.3. A solução deverá ser licenciada por número de usuários conforme tabela de quantidades.

1.1.6.1.4. A plataforma de segurança deverá ter ponto de presença próprio no Brasil, onde todos os usuários em território nacional terão suas transações processadas, incluindo todas as inspeções e aplicação de políticas de controle de acesso e segurança inline;

1.1.6.1.5. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários;

1.1.6.1.6. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto ("open source"). Os elementos ofertados não podem ser customizados;

1.1.6.1.7. A solução deverá suportar as seguintes opções de arquitetura de conectividade a plataforma de segurança, com suporte a todas as funcionalidades descritas neste certame no que tange controle de acesso e segurança à Internet e aplicações SaaS:

1.1.6.1.7.1. Com Agentes instalados nas máquinas;

1.1.6.1.7.2. Com túneis GRE (Generic Routing Encapsulation) ou IPSec, sem a necessidade de uso de agentes nas máquinas dos usuários, possibilitando saídas locais à Internet de filiais, sede e data center;

1.1.6.1.7.3. Utilização de proxy explícito via arquivos PAC (Proxy Auto-Configuration), neste caso com funcionalidades limitadas a acesso Web HTTP, HTTPS e FTP;

1.1.6.1.8. A solução de segurança, proteção de dados, controle de acesso à Internet e aplicações deverá fornecer SLA de disponibilidade de 99.999% e de latência da inspeção completa de todos os componentes, exceto detonação de arquivos do Sandbox, de no máximo 100 milissegundos em 95% das transações.

1.1.6.1.9. Toda a plataforma de segurança deverá suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud, Bloqueios de Segurança e acessos ou bloqueio de aplicações privadas via ZTNA.

1.1.6.1.10. Todas as inspeções e aplicações de políticas deverão ser realizadas na nuvem. Com exceção da verificação de postura, nenhuma inspeção de controle de acesso, segurança, DLP (Data Loss Prevention) e Firewall deverá ser realizada na máquina do usuário.

1.1.6.1.11. Todas a plataforma de segurança deverá suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud e Bloqueios de Segurança ;

1.1.6.1.12. A solução de segurança, proteção de dados, controle de acesso à Internet e aplicações SaaS, deverá suportar criação de múltiplos administradores com privilégios distintos e segmentados. Como por exemplo, políticas criadas por um administrador global, não poderão ser excluídas ou alteradas por um administrador regional ou de um departamento específico;

1.1.6.1.13. Deve suportar hierarquia entre as contas administrativas que garanta que políticas e configurações definidas por administradores com hierarquia mais alta não possam ser substituídas por administradores com hierarquia menor;

1.1.6.1.14. No caso da utilização de agentes, a gestão de como o tráfego será encaminhado à plataforma, incluindo eventuais exclusões específicas (bypass), deverá ser gerenciada de maneira centralizada em uma console Web com o contexto de usuário e grupos de usuários. Não serão aceitas soluções que requeiram alteração ou customizações diretamente na máquina do usuário;

1.1.6.1.15. O usuário deve ser capaz de reportar um problema diretamente do agente instalado no dispositivo;

1.1.6.1.16. O usuário deve ser capaz de iniciar uma captura de pacotes diretamente do agente instalado no dispositivo;

1.1.6.1.17. O agente único deve ser compatível com no mínimo os seguintes sistemas operacionais:

- **1.1.6.1.17.1.** Windows 11, 10 e 8;
- **1.1.6.1.17.2.** Fedora;
- **1.1.6.1.17.3.** Ubuntu;
- **1.1.6.1.17.4.** CentOS;
- **1.1.6.1.17.5.** MacOS 10.10 e superiores;
- **1.1.6.1.17.6.** IOS 9 e superiores;
- **1.1.6.1.17.7.** Android 8 e superiores;

1.1.6.1.18. Toda a solução deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma Microsoft Azure AD da CONTRATANTE utilizando protocolo SAML 2.0 (Security Assertion Markup Language).

1.1.6.1.19. A plataforma de segurança deverá realizar, em uma única plataforma, sem passar por inspeção em múltiplos componentes de rede dentro da nuvem do fabricante ou de terceiros, os controles de acesso e proteção de segurança ao acesso à Internet e aplicações SaaS, consolidando capacidades de soluções de SWG, CASB e FWaaS.

1.1.6.1.20. Os mecanismos de inspeção da plataforma (URL filtering, Antivirus, DLP e etc) devem verificar todo o conteúdo dos pacotes de forma simultânea e em uma única abertura;

1.1.6.1.21. A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (Security Information and Event Management) como Splunk, IBM Qradar e MS Sentinel;

1.1.6.1.22. Todas a plataforma de segurança deverá suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud e Bloqueios de Segurança;

1.1.6.1.23. A solução deve ser capaz de fornecer a visualização de logs em tempo real;

1.1.6.1.24. A solução deverá armazenar os logs de auditoria por no mínimo 4 meses;

1.1.6.1.25. Os logs de auditoria devem conter no mínimo:

- **1.1.6.1.25.1.** Ação: Importação, relatório, atualização, Patch, Login e Logout, Criação, Deleção;
- **1.1.6.1.25.2.** IP do Cliente;
- **1.1.6.1.25.3.** Interface utilizada: API, Console Administrativa;
- **1.1.6.1.25.4.** Categoria: Alerta, Backup/Restore, Gerenciamento, Controle de Acesso, Configurações de ICAP, Gerenciamento de funções, Segurança de Mobile, Controle de acesso Web, Segurança Web e configurações avançadas;
- **1.1.6.1.25.5.** Em toda alteração de configuração a solução deve ser capaz de apresentar de forma visual o que foi alterado;
- **1.1.6.1.25.6.** A solução deve mostrar de forma visual o que foi adicionado ou deletado em uma mudança de configuração;

1.1.6.2. CARACTERÍSTICAS PARA FUNCIONALIDADES DE SWG (SECURE WEB GATEWAY)

1.1.6.2.1. Suportar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.0, 1.1, 1.2 e 1.3;

1.1.6.2.2. Possibilidade de criar regras granulares de exceção a inspeção SSL/TLS, com base categorias de URL, host e domínios de destino, usuário, grupo, departamento ou tipo de browsers;

1.1.6.2.3. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente;

1.1.6.2.4. Capacidade de criar filtros de URLs com base em categorias e subcategorias, que deverão ser atualizadas constantemente pelo fabricante;

1.1.6.2.5. Suportar a criação de categorias customizadas;

1.1.6.2.6. Suportar a criação e manutenção de categorias, políticas de filtros de URL, regras de Firewall via API;

1.1.6.2.7. A solução deve fornecer mecanismo para bloquear o acesso Web a destinos hospedados em determinados países. Este bloqueio deverá ser configurado de maneira simples, apenas selecionando os países que deseja bloquear;

1.1.6.2.8. A solução deve suportar nativamente o idioma Português do Brasil em páginas de erro e bloqueio apresentadas aos usuários, além de permitir customização;

1.1.6.2.9. A solução deverá ter capacidade de criar políticas Web, granulares, com critérios utilizando nome do usuário, grupos, departamento, categorias de URL, localidades para liberação ou bloqueio de upload e/ou download de arquivos de acordo com o seu tipo. Exemplo: EXE, RAR, PKG, XLS, PDF.

1.1.6.2.10. A solução deverá prover proteção de antivírus e antimalware com base em assinatura de arquivos. Esta proteção deverá ser realizada para download e upload, e a base de dados de assinatura ser atualizada constantemente pelo fabricante;

1.1.6.2.11. A solução deverá fornecer proteção contra Ameaças Avançadas, utilizando análise estática com base em reputação do domínio, origem, idade do domínio entre outras variáveis, além de uma análise dinâmica do conteúdo Web de 100% das requisições realizada a fim de detectar potenciais riscos aos usuários, tais como injeção de JavaScript malicioso, assinaturas de roubo de cookies XSS, conteúdo ativos maliciosos, conteúdos vulneráveis de ActiveX, Phishing dentre outras;

1.1.6.2.12. A solução deverá ter atualizações constantes, minimamente diárias, de base de dados utilizada para bloqueio de segurança com base em reputação, prevenção a fraudes como Phishing, botnets, Command and Control, malware, spyware ou qualquer outro tipo de conteúdo malicioso;

1.1.6.2.13. A solução deverá detectar e bloquear assinaturas de ataques XSS (Cross Site Scripting) e de roubo de cookies dos usuários;

1.1.6.2.14. Será aceita a composição de soluções para atendimento aos itens solicitados

1.1.6.3. CARACTERÍSTICAS PARA FUNCIONALIDADES DE CONTROLE DE DNS

1.1.6.3.1. A solução de FWaaS deverá possuir a capacidade de criar políticas específicas granulares para proteção de DNS;

1.1.6.3.2. A solução deverá suportar políticas de proteção de DNS granulares contendo metadados do IdP (usuário, grupos e departamento), Localidades, Origem, Domínios Destino e tipos das requisições de DNS como A, A6, AAAA, TXT, MX, etc;

1.1.6.3.3. Para a proteção de DNS a solução deverá permitir ações como bloqueio ou redirecionar para um IP específico;

1.1.6.3.4. A solução deverá ter proteção nativa contra ataques de DNS Tunneling, permitindo bloqueio de destinos conhecidos maliciosos e mecanismo de detecção de assinaturas de ataques utilizando ferramentas conhecidas de DNS Tunneling como dnscat e iodine, independente do domínio utilizado;

1.1.6.3.5. A proteção de DNS deverá permitir bloqueio via DNS, independente do protocolo da aplicação, de domínios com baixa reputação ou com histórico de ser malicioso para Phishing, Conteúdo Malicioso e utilizados para Botnets;

1.1.6.3.6. A solução deverá ter mecanismos para bloquear requisições de DNS utilizando DOT (DNS over TLS);

1.1.6.3.7. A solução deverá detectar e redirecionar requisições de DNS utilizando DOH (DNS over HTTPS), de forma transparente, para aplicação de políticas de DNS, detalhadas nos itens acima;

1.1.6.3.8. Assim como todo o escopo do FWaaS a solução de proteção de DNS deverá suportar a implementação com o uso de agentes nas máquinas dos usuários e de túneis GRE ou IPSec da sede, filiais e data center;

1.1.6.3.9. Será aceita a composição de soluções para atendimento aos itens solicitados

1.1.6.4. CARACTERÍSTICAS PARA FUNCIONALIDADES DE VISIBILIDADE E CONTROLE DE APLICAÇÕES

1.1.6.4.1. A solução deverá com os acessos dos usuários identificar automaticamente uso de aplicações Cloud criando visibilidade em Dashboards e relatórios de Shadow IT.

1.1.6.4.2. O relatório de Shadow IT deverá permitir identificar uso de aplicações não sancionadas e com risco elevado, além de visualizar pela própria interface Web da solução quais usuários estão utilizando estas aplicações;

1.1.6.4.3. A solução deverá suportar a identificação e permitir a classificação entre aplicações sancionadas e não sancionadas pelo ÓRGÃO de no mínimo 8000 aplicações distintas. Esta base de dados deverá ser mantida e constantemente atualizada pelo fabricante e deverá conter as seguintes informações:

1.1.6.4.3.1. Categoria da aplicação

1.1.6.4.3.2. Índice que indique o risco da aplicação

1.1.6.4.3.3. Marcador se teve vazamento de dados nos últimos 3 anos

1.1.6.4.3.4. Se tem suporte a Fator Duplo de Autenticação

1.1.6.4.3.5. Se possui mecanismos de criptografia forte

1.1.6.4.3.6. Se mantém logs de auditoria

1.1.6.4.3.7. Certificações (ISO 27001, SOC 2, PCI, etc)

1.1.6.4.4. A solução deverá permitir a criação de políticas de acesso com base na classificação da aplicação SaaS realizada pela CONTRATANTE entre sancionadas e não sancionadas, índice de risco da aplicação, além de utilizar como critério adicional na política qualquer informação detalhada no item anterior;

1.1.6.4.5. A solução deverá suportar criar políticas granulares com critérios utilizando usuário, grupo departamento, localidade e ações específicas nas aplicações SaaS. Como por exemplo, aplicações de compartilhamento de arquivos ter as opções de Upload e Download como critério, em aplicações como Webmail, ter as opções de Leitura e Envia de e-mails como critério;

1.1.6.4.6. Será aceita a composição de soluções para atendimento aos itens solicitados;

1.1.7.ITEM 7 - SOLUÇÃO DE MONITORAMENTO DE EXPERIÊNCIA CONTÍNUA DOS USUÁRIOS

1.1.7.1. CARACTERÍSTICAS GERAIS

1.1.7.1.1. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço, utilizando um único agente instalado na máquina do usuário ou através de composição de soluções.

1.1.7.1.2. A nuvem do fabricante deverá ser distribuída globalmente em pelo menos 30 pontos de presença globais, incluindo o Brasil.

1.1.7.1.3. A solução deverá ser licenciada por número de usuários conforme tabela de quantidades.

1.1.7.1.4. A plataforma de segurança deverá ter ponto de presença próprio no Brasil, onde todos os usuários em território nacional terão suas transações processadas, incluindo todas as inspeções e aplicação de políticas de controle de acesso e segurança inline;

1.1.7.1.5. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários;

1.1.7.1.6. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto ("open source"). Os elementos ofertados não podem ser customizados;

1.1.7.2. FUNCIONALIDADES DE MONITORAMENTO DA EXPERIÊNCIA DO USUÁRIO:

1.1.7.2.1. A solução deverá realizar monitoramento sintético, a partir da máquina do usuário final, com testes de página Web e de Rede;

1.1.7.2.2. A console de gerenciamento deverá ser Web, e ter toda a configuração de forma centralizada;

1.1.7.2.3. A execução dos testes não deverá impactar o usuário final e deverá ser realizada em segundo plano, sendo transparente e imperceptível;

1.1.7.2.4. Quando executado testes de Web e Rede da mesma aplicação, por exemplo Microsoft Teams, a solução deverá consolidar as métricas e apresentar uma única visão da experiência do usuário ao utilizar a aplicação SaaS;

1.1.7.2.5. A solução deverá apresentar Dashboards com o status das aplicações, bem como uma mapa desta experiência distribuída em diferentes regiões do Brasil e do mundo;

1.1.7.2.6. A Geo localização deverá ser feita de maneira automática e transparente, sem nenhuma entrada de dados manual;

1.1.7.2.7. Caso o usuário esteja dentro de localizações conhecidas da solução de SWG, CASB e FWaaS, como Localidades criadas através de túneis GRE, a solução deverá identificar que trata-se de uma localidade conhecida;

1.1.7.2.8. Os testes e coleta de dados deverão acontecer no máximo a cada 15 (quinze) minutos;

1.1.7.2.9. A solução deverá coletar no mínimo as seguintes métricas de experiência:

1.1.7.2.9.1. Métricas Web:

1.1.7.2.9.1.1. Tempo total de carregamento da página

1.1.7.2.9.1.2. Tempo de resposta do Servidor

1.1.7.2.9.1.3. Tempo de resolução de DNS

1.1.7.2.9.1.4. Métricas de Rede:

1.1.7.2.9.1.5. Latência total;

1.1.7.2.9.1.6. Latência de rede até o destino final e em todos os nós no caminho;

1.1.7.2.9.1.7. Perda de pacote total;

1.1.7.2.9.1.8. Perda de pacote até o destino final e em todos os nós no caminho;

1.1.7.2.9.1.9. Caminho completo com métricas de latência e perda de pacotes. Incluindo: computador do usuário, rede wi-fi local, roteador local, saída para Internet, Fornecedora da solução SASE, empresas de telecomunicações / ISP e destino;

1.1.7.2.9.2. Métricas do dispositivo do usuário:

1.1.7.2.9.2.1. Consumo de CPU

1.1.7.2.9.2.2. Qualidade do sinal Wi-Fi

1.1.7.2.9.2.3. Memória

1.1.7.2.9.2.4. Nível de bateria

1.1.7.2.9.2.5. Estatísticas de I/O de discos

1.1.7.2.9.2.6. Sistema Operacional, Descrição do hardware, DNS utilizado, IP público e IP externo utilizado

1.1.7.2.9.2.7. Histórico de eventos no sistema operacional, como troca de rede wi-fi, troca de IP, etc;

1.1.7.2.10. Utilizando as métricas do dispositivo do usuário, testes Web e de Rede, a solução deverá ter um mecanismo simples de identificar a experiência do usuário em uma aplicação, atribuindo um índice que indica se a experiência está Boa, Razoável ou Ruim;

1.1.7.2.11. A solução deverá suportar o monitoramento de Websites na Internet, aplicações SaaS e aplicações privadas fornecidas pela solução de ZTNA;

1.1.7.2.12. A solução deverá suportar a criação de alertas customizáveis com notificação por e-mail;

1.1.7.2.13. A solução deverá manter o histórico da experiência de todos os usuários, por no mínimo 48 (quarenta e oito) horas;

1.1.7.2.14. Será aceita a composição de soluções para atendimento aos itens solicitados;

1.1.8.ITEM 8 - SOLUÇÃO PARA ACESSO SEGURO A APLICAÇÕES PRIVADAS

1.1.8.1. CARACTERÍSTICAS GERAIS

1.1.8.1.1. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço, utilizando um único agente instalado na máquina do usuário ou através de composição de soluções.

1.1.8.1.2. A nuvem do fabricante deverá ser distribuída globalmente em pelo menos 30 pontos de presença globais, incluindo o Brasil.

1.1.8.1.3. A solução deverá ser licenciada por número de usuários conforme tabela de quantidades.

1.1.8.1.4. A plataforma de segurança deverá ter ponto de presença no Brasil, onde todos usuários em território nacional terão suas transações processadas;

1.1.8.1.5. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários;

1.1.8.1.6. O Datacenter do fabricante localizado no Brasil deve possuir no minímo 2 links com velocidade superior a 50GB no principal ponto de troca do Brasil (IX.BR);

1.1.8.1.7. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto ("open source"). Os elementos ofertados não podem ser customizados;

1.1.8.1.8. Todas as inspeções e aplicações de políticas deverão ser realizadas na nuvem. Com exceção da verificação de postura, nenhuma inspeção de controle de acesso deverá ser realizada na máquina do usuário.

1.1.8.1.9. No caso da utilização de agentes, a gestão de como o tráfego será encaminhado à plataforma, incluindo eventuais exclusões específicas (bypass), deverá ser gerenciada de maneira centralizada em uma console Web com o contexto de usuário e grupos de usuários. Não serão aceitas soluções que requeiram alteração ou customizações diretamente na máquina do usuário;

1.1.8.1.10. O usuário deve ser capaz de reportar um problema diretamente do agente instalado no dispositivo;

1.1.8.1.11. O agente único deve ser compatível com no mínimo os seguintes sistemas operacionais:

1.1.8.1.11.1. Windows 11, 10 e 8;

1.1.8.1.11.2. Fedora;

1.1.8.1.11.3. Ubuntu;

1.1.8.1.11.4. CentOS;

1.1.8.1.11.5. MacOS 10.10 e superiores;

1.1.8.1.11.6. IOS 9 e superiores;

1.1.8.1.11.7. Android 8 e superiores;

1.1.8.1.12. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma Microsoft Azure AD da CONTRATANTE utilizando protocolo SAML 2.0 (Security Assertion Markup Language).

1.1.8.2. Acesso a aplicações privadas

1.1.8.2.1. A solução deverá fornecer acesso remoto a aplicações e recursos internos da CONTRATANTE, com segurança, validação de identidade, tunelamento encriptado, segregação de aplicações, verificação de postura e conexão direta com privilégio mínimo;

1.1.8.2.2. A solução deve habilitar uma arquitetura de privilégio mínimo, Zero Trust, definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque;

1.1.8.2.3. A solução deverá ser na nuvem e ter apenas o componente que irá viabilizar a conexão (conector ou publicador) instalado dentro do Data Center da CONTRATANTE em uma, ou mais, máquinas virtuais. Este componente deverá:

1.1.8.2.4. Ter arquitetura de alta disponibilidade e realizar o balanceamento de carga automaticamente, sem depender de nenhum componente de rede da infraestrutura da CONTRATANTE

1.1.8.2.5. Não ter uma superfície de ataque exposta na Internet, não tendo nenhum IP público ou nenhuma necessidade de conexões de entrada da Internet para o componente

1.1.8.2.6. Toda a conexão deverá ser apenas de saída, do componente com destino a nuvem do fabricante

1.1.8.2.7. Os conectores ou publicadores deverão atualizar suas versões de forma automática e realizar suas atualizações em janelas pré-definidas pela CONTRATANTE (ex: Domingo às 4 AM) de forma 100% automatizada, sem causar interrupção dos serviços e sem intervenção do administrador;

1.1.8.2.8. Permitir ser instalado de forma flexível em qualquer ponto da rede da CONTRATANTE, como por exemplo atrás de uma NAT (Network Address Translation)

1.1.8.2.9. Não criar um ponto único de conexão a rede da CONTRATANTE, sendo possível a implementação de múltiplos conectores ou publicadores em pontos da rede, data centers ou nuvem distintas, fornecendo ao usuário o acesso direto aos recursos com menor latência possível de forma dinâmica;

1.1.8.2.10. Cada instância de conector ou publicador deverá suportar no mínimo 500mb de banda passante para acesso às aplicações internas;

1.1.8.2.11. Permitir o usuário a conectar em aplicações distintas simultaneamente utilizando conectores ou publicadores em pontos da rede distintos, priorizando sempre a melhor experiência do usuário;

1.1.8.2.12. A plataforma deverá permitir a descoberta automatizada de novas aplicações que não foram préviamente provisionada aos usuários explicitamente;

1.1.8.2.13. Os conectores ou publicadores deverão ser independentes, não exigindo conectividade interna completa a todos os recursos privados. Sendo possível, por exemplo, fornecer acesso a aplicações ou recursos simultaneamente aos usuários em múltiplos Data Centers ou Nuvem, mesmo que estes Data Centers ou Nuvem não tenham conexão entre eles;

1.1.8.2.14. A solução deverá autenticar o usuário em um provedor de identidade (IdP) e com base em identidade, políticas granulares, segmentação de aplicações e posturas específicas fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, Aplicações Client-to-Server, Compartilhamento de Arquivos, etc) de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando um túnel encriptado que conectará o usuário até a aplicação e não a rede da CONTRATANTE.

1.1.8.2.15. A solução deve suportar múltiplos IDPs;

1.1.8.2.16. A solução não deve operar como uma VPN fornecendo um IP da rede local, e sim conectar o usuário direto, após validação de política de identidade, postura e políticas de acesso, aos recursos e aplicações com túneis encriptados específicos;

1.1.8.2.17. Os usuários remotos, não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis;

1.1.8.2.18. A definição de aplicações ou segmentos de aplicações deverá ter a flexibilidade de suportar hostname (FQDN), IP ou domínio com wildcard, como por exemplo (*.rede.local)

1.1.8.2.19. A solução deve fazer com que cada solicitação do usuário flua por meio de políticas contextual para autenticação e autorização consistentes, além de fornecer um ponto de monitoramento e registro unificado;

1.1.8.2.20. A solução deverá utilizar túneis encriptados TLS ou DTLS, versão 1.2 ou 1.3;

1.1.8.2.21. Todas as comunicações entre os componentes da solução e a infraestrutura em nuvem do fabricante devem mutualmente utilizar certificados pinados;

1.1.8.2.22. A solução deve ser blindada contra ataques de "Man-in-the-middle"(MITM);

1.1.8.2.23. A solução deverá suportar controle granular de timeout de autenticação baseado em políticas específicas de acordo com o recurso ou aplicação acessada. Como por exemplo, para acesso ao ERP o usuário deverá ter se autenticado na última 1 hora pelo menos, caso negativo, solicitar autenticação novamente, para as demais aplicações o usuário deverá ter se autenticado nos últimos 3 dias;

1.1.8.2.24. A solução deve permitir o acesso a quais recursos por meio de uma estrutura de política simples que leva em consideração qualquer atributo do usuário fornecido pelo IdP, inclusive customizados, e o estado do dispositivo;

1.1.8.2.25. A solução deve trazer o monitoramento da atividade dos usuários, dando às equipes de TI uma maneira de monitorar e gerenciar facilmente todas as atividades de forma granular, entendendo qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso, status da postura localização do usuário;

1.1.8.2.26. A solução deve usar o painel Web para criar e editar políticas com facilidade. O portal de gestão central deve trazer:

- **1.1.8.2.26.1.** Controle de acesso centralizado
- **1.1.8.2.26.2.** Gestão de políticas
- **1.1.8.2.26.3.** Configuração de postura
- **1.1.8.2.26.4.** Registro de atividades detalhados e seus metadados como usuário, localidade, postura, IP de origem, aplicação destino, política de acesso que concedeu ou negou o acesso
- **1.1.8.2.26.5.** Status da estrutura que suporte a solução como conectores ou publicadores
- **1.1.8.2.26.6.** Status do processo de atualização automatizada dos conectores e publicadores
- **1.1.8.2.26.7.** Status das aplicações que deverão ser monitoradas se estão disponíveis ou não
- **1.1.8.2.26.8.** Gerenciar a segmentação do acesso ou recursos
- **1.1.8.2.26.9.** Suportar a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem nenhuma alteração ou customização no seu cliente original
- **1.1.8.2.26.10.** Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (Ex: Aplicações Administrativas)

1.1.8.2.27. A solução deverá suportar a gestão de políticas de acesso via API;

1.1.8.2.28. A solução deverá suportar diferentes tipos de validação de postura. O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux, iOS e Android), sendo requerido que no mínimo deverá suportar 2 dos tipos abaixo por plataforma:

1.1.8.2.28.1. Validação da presença de um Antivírus

1.1.8.2.28.2. Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico

1.1.8.2.28.3. Validação de Certificado confiável no dispositivo

1.1.8.2.28.4. Validação de qualquer processo executando na máquina, incluindo a validação da assinatura do seu fabricante

1.1.8.2.28.5. Validação de máquina no domínio

1.1.8.2.28.6. Validação de disco encriptado

1.1.8.2.28.7. Validação de Registro de chave no Windows

1.1.8.2.28.8. Validação de presença de um arquivo

1.1.8.2.28.9. Exigência de uma versão mínima do Sistema Operacional

1.1.8.2.28.10. Detectar alterações não autorizadas em dispositivos móveis

1.1.8.2.29. A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação. Desta maneira permitindo criar maiores restrições a aplicações mais críticas ao negócio e menos restritas a aplicações de suporte a TI. Como por exemplo, para acessar o ERP da CONTRANTANTE será necessário estar autenticado, ser do grupo de finanças, está executando o Anti-Virus no desktop, ter o certificado da CONTRATANTE na máquina e estar dentro do domínio do AD. Para acessar a aplicação de suporte a TI, será exigido apenas estar autenticado.

1.1.8.2.30. O agente de comunicação deve permitir a configuração de túneis antes mesmo do logon do usuário para permitir serviços do Active Directory pré-logon.

1.1.8.2.31. A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação. Desta maneira permitindo criar maiores restrições a aplicações mais críticas ao negócio e menos restritas a aplicações de suporte a TI. Como por exemplo, para acessar o ERP da CONTRANTANTE será necessário estar autenticado, ser do grupo de finanças, está executando o Anti-Virus no desktop, ter o certificado da CONTRATANTE na máquina e estar dentro do domínio do AD. Para acessar a aplicação de suporte a TI, será exigido apenas estar autenticado.

1.1.8.2.32. A solução deverá também oferecer, na mesma plataforma sem necessidade de instalação de componentes adicionais, o suporte a usuários sem o uso de agentes para fornecer acesso a aplicações privadas com protocolo Web utilizando tecnologia de Proxy Reverso ou similar.

1.1.8.2.33. A solução deve ser capaz de fornecer visualização de eventos em tempo real;

1.1.8.2.34. Deve fornecer informações granulares sobre as atividades dos usuários contendo no mínimo:

1.1.8.2.34.1. A hora que a conexão se iniciou;

1.1.8.2.34.2. A hora final da conexão;

1.1.8.2.34.3. Número total de Bytes;

1.1.8.2.34.4. A política de Acesso associada;

1.1.8.2.34.5. Ação tomada;

1.1.8.2.34.6. Informações do usuário: IP, Localização e nome do usuário;

1.1.8.2.34.7. Informações da aplicação: Porta e protocolo;

1.1.8.2.35. Será aceita a composição de soluções para atendimento aos itens solicitados;

1.1.9.ITEM 9 - SOLUÇÃO DE SEGURANÇA DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM

1.1.9.1. CARACTERÍSTICAS GERAIS

1.1.9.1.1. A contratante deverá optar por licenciamento da solução para repositórios de nuvem Microsoft 365 ou Google Drive com quantitativo a ser definido no momento da contratação;

1.1.9.1.2. A solução deverá coletar trilha de auditoria de acesso dos usuários aos dados armazenados no repositório de nuvem monitorado;

1.1.9.1.3. A solução deverá permitir a filtragem gráfica da trilha de auditoria;

1.1.9.1.4. A solução deverá normalizar e analisar permissões dos usuários aos dados da nuvem corporativa coletiva;

1.1.9.1.5. A solução deverá apresentar todos os usuários que têm permissões e quais permissões cada usuário tem em uma pasta ou arquivo armazenado no repositório;

1.1.9.1.6. A solução deverá apresentar todos os dados que um usuário selecionado tem acesso e qual tipo de permissão;

1.1.9.1.7. A solução deverá demonstrar dados sensíveis compartilhados externamente e expostos publicamente;

1.1.9.1.8. A solução deverá descobrir configurações incorretas no repositório;

1.1.9.1.9. A solução deverá apresentar métricas e configurações incorretas que podem afetar a segurança do ambiente, como: pastas e repositórios expostos publicamente, dados inativos;

1.1.9.1.10. A solução deverá fornecer recomendações de como corrigir rapidamente configurações incorretas do ambiente monitorado.

1.1.9.1.11. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário.

1.1.9.1.12. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos.

1.1.9.1.13. A solução deverá ter suas funcionalidades de descoberta de dados sensíveis para repositórios de nuvem Google ou Microsoft.

1.1.9.1.14. As informações produzidas pela solução sobre dados sensíveis devem ser disponibilizadas em forma de relatórios.

1.1.9.1.15. As consultas aos logs de auditoria e relatórios devem suportar filtros de classificação de dados sensíveis.

1.1.9.1.16. A solução deverá identificar atividades de contas pessoais externas acessando os dados armazenados nos repositórios de nuvem;

1.1.9.1.17. A solução deve demonstrar em sua console a quantidade de dados sensíveis descobertos nos arquivos e pastas.

1.1.9.1.18. A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.

1.1.9.1.19. A ferramenta deve permitir integração com ferramentas do DLP (Data Loss Prevention) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução.

1.1.9.1.20. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;

1.1.9.1.21. A solução deve ser capaz de identificar dados que possuam informações referente a Lei de Geral de Proteção de Dados (LGPD) como por exemplo: nome, CPF, passaporte, religião, gênero, nacionalidade, entre outros.

1.1.9.1.22. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

1.1.9.1.23. Nos alertas em tempo real, deve ser possível configurar para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva.

1.1.9.1.24. Os alertas poderão ser iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada;

1.1.9.1.25. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;

1.1.9.1.26. O dashboard deve apresentar os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;

1.1.9.1.27. Os alertas devem ser gerados e podem ser encaminhados de forma automática através de SMTP;

1.1.9.1.28. Deve ser possível realizar a remediação de algumas ações como: remoção de links públicos, remoção de links compartilhados com toda a organização;

1.1.9.1.29. A solução deverá permitir o agendamento das execuções das regras de remediação automatizada de forma que elas possam ser executadas recorrentemente ou uma única vez;

1.1.9.1.30. A solução deverá permitir a definição de limites de horário para execução das regras;

1.1.9.1.31. A solução deve apresentar em relatório o resultado da execução das regras com o caminho da pasta e arquivo, a ação executada sobre a permissão, os grupos de segurança e usuários afetados, a permissão afetada e erros e alertas da execução;

1.1.9.1.32. A solução deverá permitir a extração dos relatórios de execução das regras de remediação;

1.1.9.2. FUNCIONAMENTO GERAL

1.1.9.2.1. Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução de auditoria deverá ser de um único fabricante;

1.1.9.2.2. A solução deve disponibilizar console web para acesso da solução através das estações de trabalho dos usuários autorizados;

1.1.9.2.3. A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention) e SIEM.

1.1.9.2.4. Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo não deve impactar na disponibilidade dos servidores ou serviços;

1.1.9.2.5. O agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;

1.1.9.2.6. A solução deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, podendo, desta forma, ser utilizada por diferentes equipes com variadas demandas de atividades e com acesso restrito a diferentes funções.

1.1.9.2.7. Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares.

1.1.9.2.8. A solução deve suportar a utilização de servidores virtualizados para os componentes;

1.1.9.2.9. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;

1.1.9.2.10. A solução deverá fazer recomendações de melhores práticas a serem aplicadas no ambiente;

1.1.9.3. RELATÓRIOS

1.1.9.3.1. A solução ofertada deve gerar relatórios em diversos formatos de arquivos;

1.1.9.3.2. A ferramenta deve permitir que relatórios sejam extraídos sob demanda uma única vez ou agendados e enviados com frequência definida;

1.1.9.3.3. A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico ou para um compartilhamento no servidor de arquivos;

1.1.9.3.4. A ferramenta deve fornecer relatório de todas as permissões de determinado usuário nos repositórios monitorados.

1.1.9.3.5. A ferramenta deve fornecer relatório de todos os usuários com permissões em determinada pasta.

1.1.9.3.6. A ferramenta deve fornecer relatório dos acessos aos arquivos;

1.1.9.3.7. Fornecer relatórios de dados e usuários inativos;

1.1.9.3.8. A solução deve fornecer relatório de histórico de permissões;

1.1.9.3.9. A solução deve fornecer relatório de histórico de membros de grupos de segurança;

1.1.9.3.10. A solução deve oferecer relatórios de estatísticas, métricas e gráficos com informações sobre usuários, grupos, pastas e permissões ao longo de determinado período;

1.1.9.3.11. Fornecer relatório dos alertas de comportamento anômalo identificados;

1.1.9.3.12. A solução deve fornecer relatório com as recomendações de revogação de permissão gerados pela análise comportamental realizada sobre os usuários e recursos monitorados;

1.1.9.3.13. A solução deve oferecer relatório de estatística de acesso, utilização por tipo de arquivos, eventos por usuários e distribuição por tipos de eventos;

1.1.9.3.14. A solução deve fornecer relatório de auditoria das ações dos usuários na console;

1.1.9.4. CONTROLE DE ACESSOS (PERMISSIONAMENTO):

1.1.9.4.1. A solução deverá exibir para cada pasta dos recursos monitorados a visualização gráfica e interativa das listas de controle de acesso incluindo grupos, subgrupos e seus respectivos membros;

1.1.9.4.2. A interface gráfica deverá permitir a busca por um usuário ou grupo e apresentar graficamente seus níveis de permissão nos diretórios dos recursos monitorados. Esta visibilidade deve incluir herança de permissão ativa/desativada e indicação de compartilhamento;

1.1.9.4.3. A solução deve permitir uma pré-visualização das alterações de permissionamento pretendidas de maneira gráfica antes da aplicação em produção. Esta pré-visualização deve demonstrar os impactos nos grupos e usuários em relação a suas permissões nos diretórios monitorados;

1.1.9.5. REGISTRO DE EVENTOS

1.1.9.5.1. A solução deve coletar o log das plataformas monitoradas de forma contínua e automática e normatizar essas informações em banco de dados.

1.1.9.5.2. A solução deve apresentar todos os logs de todos os usuários na mesma console de visibilidade de permissionamento da plataforma monitorada;

1.1.9.5.3. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;

1.1.9.5.4. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;

1.1.9.5.5. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;

1.1.9.5.6. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação.

1.1.10. ITEM 10 - SOLUÇÃO DE PROTEÇÃO E SEGURANÇA DE DADOS

1.1.10.1. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante. Todos os componentes de software descritos deverão ser de um único FABRICANTE.

1.1.10.2. Todos os componentes do software de Backup e Restore deverão ser do mesmo fabricante, integrados e que ofereçam um módulo único de gerenciamento. Não será aceito mais de um software de Backup e Restore para atendimento dos requisitos técnicos especificados.

1.1.10.3. A solução ofertada deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do fabricante.

1.1.10.4. Todas as funcionalidades e requisitos elencados neste documento, independentemente de qualquer quantidade de utilização do referido serviço, deve estar disponível sem nenhum tipo de cobrança adicional.

1.1.10.5. Deverão ser fornecidas licenças na modalidade Front End Terabyte.

1.1.10.6. A licença deverá incluir todas as funcionalidades solicitadas no presente termo, com suporte para backup, restore e tecnologia de desduplicação global de dados, onde o licenciamento deverá possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres e suportar toda a infraestrutura da CONTRATANTE detalhada no Edital, sem nenhum ônus a durante a vigência do contrato;

1.1.10.7. A solução de Proteção de Dados a ser ofertada deverá atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças que forem necessárias para entrega 100% funcional da solução Arquitetura e Características Gerais do Software

1.1.10.8. Possuir arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:

1.1.10.8.1. Camada de gerência.

1.1.10.8.2. Camada do serviço de mídia/unidade de disco de retenção dos dados.

1.1.10.8.3. Camada de clientes/agentes multiplataforma de backups.

1.1.10.9. Deve possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto.

1.1.10.10. A solução de Bakckup e Recovery deverá permitir a possibilidade de múltiplas políticas de disaster recovery para prevenir perda de dados e cópia automática do catálogo do backup, sincronização entre as cópias do catálogo do backup, replicação entre appliances no mesmo domínio de backup e replicação entre appliances em domínios de backup diferentes.

1.1.10.11. Deve possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dos dados.

1.1.10.12. Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatalogar as imagens de backup.

1.1.10.13. Deve fazer uso de banco de dados relacional para guardar o catálogo de Jobs, arquivos e mídias dos backups.

1.1.10.14. Deve suportar servidor de gerência e catálogo instalados em conjunto nas seguintes plataformas: Linux e Windows. Não serão aceitos catálogos instalados em plataformas (sistemas operacionais) diferentes da utilizada no servidor de gerência.

1.1.10.15. Deverá permitir a configuração de servidores de gerência e catálogo no mesmo servidor ou instância, e suportar arquitetura em cluster para promover alta-disponibilidade dos serviços de gerenciamento. A implementação dos serviços de gerenciamento, catálogo e cluster deverá ser suportado nas seguintes plataformas: Red Hat Enterprise Linux, Suse Enterprise Linux e Windows;

1.1.10.16. Deve suportar servidores movimentadores de dados nas seguintes plataformas: Linux e Windows.

1.1.10.17. Os servidores movimentadores de dados devem suportar balanceamento de carga para distribuir a carga entre eles de forma automática.

1.1.10.18. Os servidores movimentadores de dados devem suportar configuração de recurso automático de failover, ou seja, permitir a configuração de mais de um servidor movimentador de dados em uma política de proteção, de forma que a indisponibilidade de um servidor seja suprida por outro servidor movimentador de dados disponível de forma automática. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

1.1.10.19. Deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.

1.1.10.20. Deve ser capaz de gerenciar múltiplos e diferentes dispositivos de backup (bibliotecas de fitas, drives de backup, dispositivos de disco com e sem desduplicação), conectados localmente (Direct Attached) e compartilhados entre múltiplos servidores da camada de mídia via SAN (Storage Area Network).

1.1.10.21. Possuir a capacidade de escrever múltiplos fluxos de dados provenientes de servidores distintos (multiplexação), divididos em blocos de tamanhos constantes em um único dispositivo físico de gravação.

1.1.10.22. Possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (multiple streams).

1.1.10.23. Possuir a capacidade de reiniciar backups e retores a partir do ponto de falha, após a ocorrência da mesma.

1.1.10.24. Deve possuir mecanismo de instalação e atualização de clientes e agentes de backup de forma remota, por intermédio da interface de gerenciamento, permitindo a instalação de múltiplos clientes de backup simultaneamente.

1.1.10.25. Possuir a capacidade de realizar download e instalação de atualizações, de forma automática, no servidor de backup e clientes.

1.1.10.26. Possuir ambiente de gerenciamento de backup e restore via interface gráfica e linha de comando.

1.1.10.27. Possuir função de agendamento do backup através de calendário.

1.1.10.28. Possuir interface gráfica para gerenciamento, monitoramento e criação de políticas de backup e restore.

1.1.10.29. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.

1.1.10.30. Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos;

1.1.10.31. Possuir função para definição de prioridades de execução de Jobs de backup;

1.1.10.32. Deverá permitir o agendamento de jobs de backup, sem utilização de utilitários de agendamento dos hosts;

1.1.10.33. Deverá permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens;

1.1.10.34. Possuir a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética;

1.1.10.35. Possuir políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dados de backup entre camadas através do seu ciclo de vida;

1.1.10.36. Permitir a realização do backup completo de servidor para recuperação de desastres;

1.1.10.37. Permitir restaurar o backup de recuperação de desastres para hardware diferente do original - para ambiente Windows;

1.1.10.38. Permitir o controle da banda de tráfego de rede durante a execução do backup e/ou do restore;

1.1.10.39. Suportar integração com OST (OpenStorage) Disk Appliances através de OpenStorage API;

1.1.10.40. Ser capaz de recuperar dados para servidores diferentes do equipamento de origem;

1.1.10.41. Ser capaz de utilizar qualquer tecnologia utilizada pela Solução de Armazenamento como destino dos backups seja armazenamento diretamente anexado (DAS), armazenamento em rede NAS ou rede SAN;

1.1.10.42. Possuir a função de Disk Staging, ou seja, que permita o envio dos dados para disco e posteriormente do disco para outro tipo de mídia (disco ou fita);

1.1.10.43. Permitir que Logical Unit Numbers (LUNs) sejam apresentadas aos servidores da camada de mídia como destino para realização de backups;

1.1.10.44. Permitir o compartilhamento de LUNs entre vários servidores de mídia de mesmo sistema operacional;

1.1.10.45. A Solução de Proteção de Dados deve suportar e estar licenciada para backup e restore de file systems montados em dispositivos Network-Attached Storage (NAS) através do suporte ao protocolo NDMP versão 4 ou superiores;

1.1.10.46. Para proteção dos dados em dispositivos NAS Network-Attached Storage deverá ser fornecido licenciamento na unidade de TB (Terabyte)

1.1.10.47. Permitir integração do controle de acesso com sistemas de diretório NIS, NIS+ e Active Directory;

1.1.10.48. Permitir a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informações de catálogo da imagem de origem para o catálogo do destino, de forma automática e sem a necessidade de licenciamento adicional.

1.1.10.49. Possuir Interface única para gerenciamento de todos os servidores independente do S.O que hospeda esse serviço (Windows, Linux); ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remotas.

1.1.10.50. Deverá implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho

1.1.10.51. A Solução de Backup deverá permitir operações de Backup e Restore através de rede local (LAN_based e Storage Area Network SAN_based ou LAN_free);

1.1.10.52. Deverá permitir a verificação da integridade do conteúdo das fitas por software;

1.1.10.53. Deverá permitir liberação das fitas magnéticas quando todos os arquivos contidos nas mesmas tenham suas datas de retenção expiradas;

1.1.10.54. As fitas liberadas devem ficar disponíveis automaticamente para uso de outras tarefas de backup;

1.1.10.55. A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais (clientes); bem como operações de recuperação bare metal.

1.1.10.56. Deverá permitir a criação de imagens de servidores físicos, Linux e Windows, para recuperação de desastres (funcionalidade conhecida como bare metal restore de forma nativa, i.e., sem a utilização de software de terceiros;

1.1.10.57. Para servidores Windows, deverá ser possível a recuperação das imagens de recuperação de desastres mesmo em um hardware diferente do original ou em ambiente virtual.

1.1.10.58. A funcionalidade de baremetal especificada anteriormente deverá suportar em um único servidor de gerência ou servidor de mídia várias versões de Windows – Windows 2012, 2012R2, 2016, 2019).

1.1.10.59. Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção;

1.1.10.60. Deverá possuir a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre;

1.1.10.61. Deverá possuir capacidade de realizar desduplicação de dados na camada no cliente, servidor de backup e appliances de desduplicação. A solução deverá permitir a desduplicação de qualquer capacidade (de acordo com o volume identificado e licenciado) e em qualquer forma de desduplicação (cliente, servidor de backup e appliances) nativamente, não sendo aceitos composições de produtos;

1.1.10.62. Deverá suportar desduplicação de blocos na origem (client-side), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full;

1.1.10.63. Deverá suportar desduplicação Global de blocos de tamanho fixo e variável.

1.1.10.64. Não serão aceitas soluções de desduplicação Global parciais, aplicadas por Jobs, políticas de backup independentes ou apenas para cenários de replicação de dados via WAN.

1.1.10.65. A solução de backup deverá ser capaz de gerenciar a réplica do backup desduplicado entre appliances de desduplicação.

1.1.10.66. Deverá possuir a capacidade de desduplicação global de dados no nível de segmentos ou blocos de dados repetidos, entre ambientes físicos e virtuais, mesmo em localidades remotas. Não serão aceitas soluções que utilizem mecanismos de desduplicação parcial aplicados a ambientes isolados ou por jobs.

1.1.10.67. Permitir o envio de dados desduplicados para a nuvem, caso seja necessário o fornecimento de recusros adicionais de software, hardware e licenciamento os mesmos deverão constar detalhados na proposta;

1.1.10.68. Deverá possuir algoritmo hash de desduplicação SHA-2;

1.1.10.69. Deverá possuir a capacidade de desduplicação de dados no nível de segmentos ou blocos de dados repetidos de ambientes Oracle;

1.1.10.70. Deverá suportar desduplicação de blocos na origem (client-side), para ambientes Oracle;

1.1.10.71. Deverá permitir ativar o recurso de desduplicação Global em volumes apresentados via SAN, DAS e iSCSI para servidores Windows, Linux e Unix;

1.1.10.72. Deverá possuir a capacidade de Replicação de Dados entre "pools" de desduplicação de maneira otimizada, enviando somente blocos únicos.

1.1.10.73. Deverá possuir a capacidade de realizar balanceamento de carga automático entre servidores ou appliances de desduplicação;

1.1.10.74. Deverá possibilitar a distribuição automática de carga entre os servidores que executarão o serviço de proteção de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de backup da solução. Em caso de falha de um dos servidores de backup, o cliente automaticamente irá encaminhar seus dados através de outro servidor de backup ativo. Esta funcionalidade deverá ser nativa do produto, não sendo admitidas soluções baseadas em softwares de cluster de terceiros;

1.1.10.75. Deverá possuir a capacidade de criptografar os dados armazenados de forma desduplicada;

1.1.10.76. As políticas de ciclo de vida da informação devem permitir a replicação das imagens de backup de forma otimizada, fazendo o uso da tecnologia de desduplicação de dados da solução no mesmo site ou entre sites distintos;

1.1.10.77. Deverá fazer uso de tecnologia de replicação dos dados (não somente os dados protegidos – imagens de backup – mas também do catálogo do software de backup necessário para a recuperação do dado) do site principal para o site de desastre, de forma que em um evento de desastre, os sites sejam independentes no processo de recuperação.

1.1.10.78. Deverá possuir tecnologia de desduplicação de dados inline por padrão;

1.1.10.79. Deverá permitir que depois de um backup full inicial, os backups subsequentes sejam feitos apenas através do envio das diferenças desduplicadas e que esses backups sejam consolidados como se fosse um backup full com a última data de envio.

1.1.10.80. Deverá possuir a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre;

1.1.10.81. Deverá possuir a capacidade de proteção da base de hashes de desduplicação com cópia externa;

1.1.10.82. Para facilitar o processo de verificação de pré-requisitos e compatibilidade, o fabricante deverá possuir mecanismo público de geração de lista de checagem que, através da informação do pacote a ser instalado, do sistema operacional alvo da instalação, gere uma lista que contenha:

1.1.10.83. Patches do Sistema Operacional e de dispositivos de hardware que porventura necessitem estar instalados;

1.1.10.84. Componentes do produto suportados para instalação ou uso no Sistema Operacional em questão;

1.1.10.85. Requerimentos de Hardware para instalação do produto no Sistema Operacional em questão;

1.1.10.86. Componentes de Hardware compatíveis;
1.1.10.87. Compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System);
1.1.10.88. Possíveis correções e atualizações adicionais disponíveis para o funcionamento do produto no Sistema Operacional alvo.
1.1.10.89. Deverá possuir e implementar o fator duplo de autenticação - 2FA para o console de administração gráfica e linha de comando por meio do provedor de identidade baseado em SAML ou cartões inteligentes CAC / PIV ou certificados de usuário Criptografia
1.1.10.90. Deverá permitir escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado ou no servidor de backup;
1.1.10.91. Deverá possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia;
1.1.10.92. Deverá implementar criptografia TLS 1.2 ou superior durante o tráfego dos dados (in-transit) e no armazenamento (at-rest) em todos os backups, restaurações, replicação automática de imagens e desduplicação.
1.1.10.93. Deverá implementar criptografia (in-transit) para os metadados de catálogo de backup;
1.1.10.94. Deverá possibilitar enviar notificações, quando configurado, dos eventos por e-mail;
1.1.10.95. Possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:
1.1.10.96. Data e hora da operação, Usuário que realizou a operação, Ação realizada (em caso de modificação de configurações, informar qual a configuração anterior e a modificação realizada).
1.1.10.97. Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica e linha de comando.
1.1.10.98. Deverá prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos jobs.
1.1.10.99. Deverá suportar operações de backup e restore em paralelo;
1.1.10.100. Deverá permitir encadear Jobs para que um só comece após outro ter terminado;
1.1.10.101. Deverá possuir a funcionalidade de proteção contínua de dados (CDP) para todo o ambiente VMware com no mínimo os seguintes requisitos:
1.1.10.102. Não poderá impactar as VMs durante a execução da proteção contínua de dados (CDP)
1.1.10.103. Deverá proteger continuamente os dados das VMs do ambiente VMware e fornecer backup de baixo RPO (até 30 minutos) por meio de interface de administração java ou web.
1.1.10.104. Deverá oferece suporte para backup com acelerador para armazenamento baseado em disco de desduplicação, além de restauração de arquivo único sem agente.
1.1.10.105. Deverá ser possível limitar os recursos com base no gateway CDP.
1.1.10.106. Deverá suportar API e RBAC para a proteção contínua dos dados e gerenciamento de gateway.
1.1.10.107. Deverá suportar armazenamento nos cloud storages: Amazon S3, Microsoft Azure e Google Cloud Storage.
1.1.10.108. Deverá suportar desduplicação de dados em Clouds a fim de reduzir o consumo de rede e armazenamento em nuvem, caso seja necessário o fornecimento de recusros adicionais de software, hardware e licenciamento os mesmos deverão constar detalhados na proposta;
1.1.10.109. Deverá possuir a capacidade de gravar informações de catálogo nos backups enviados para, ao menos, Microsoft Azure e Amazon S3;
1.1.10.110. Deverá ter a capacidade de recuperar as imagens de backup gravadas em, ao menos, Microsoft Azure e Amazon S3 convertendo em instancias na nuvem (IaaS) em caso de desastre no ambiente on-premises;
1.1.10.111. Deverá permitir a orquestração de sistemas físicos e virtuais de forma automatizada para recuperação de desastres com no mínimo:
1.1.10.112. Permitir a recuperação de desastres orquestrada, automatizada e em escala para o próprio data center, ambientes híbridos e multicloud.
1.1.10.113. Permitir a recuperar sistemas locais na nuvem com visibilidade direta e integrado ao software de backup.
1.1.10.114. Permitir a recuperação de desastres orquestrada para ambientes Oracle.
1.1.10.115. Permitir a recuperação automatizada e orquestrada para aplicativos de várias camadas na nuvem e no local com APIs para otimizar o tempo e os recursos.

1.1.10.116. Prover meios automáticos de garantir a consistência do backup a nível de aplicação, ou seja, ser capaz de automatizar a restauração de uma máquina virtual e executar ações de testes previamente programadas para aquela determinada aplicação de forma a garantir que o backup está consistente.

1.1.10.117. Deverá ter a capacidade de testar a consistência do backup, emitindo relatório de auditoria para garanti a capacidade de recuperação seguintes parâmetros: sistema operacional, aplicação e máquina virtual.

1.1.10.118. Deve permitir a replicação dos dados de VMware para VMware, VMware para AWS, VMware para Azure, VMware para Google, Hyper-V para AWS, Hyper-V para Azure, Hyper-V para Hyper-V, Hyper-V para Google;

1.1.10.119. Deve permitir a recuperação granular de desastres, ou seja, deverá ser possível realizar o failover e migração de máquinas virtuais, aplicações individuais, um serviço composto por múltiplos componentes e até mesmo do site inteiro;

1.1.10.120. Deve suportar o failover e migração de máquinas virtuais para virtuais, físicas para virtuais, físicas para nuvem e máquinas virtuais para nuvem;

1.1.10.121. Deve automatizar a utilização de recursos na nuvem de maneira dinâmica, para otimização de custos;

1.1.10.122. Deve automatizar a criação de componentes da solução na nuvem conforme a necessidade, removendo quando deixarem de ser necessários;

1.1.10.123. Deve automatizar operações de resiliência incluindo: testes de recuperação/simulação, migrações, failover e failback;

1.1.10.124. Deve possuir funcionalidade para simulação de desastres, ou seja, permitir a verificação de uma operação de failover para o site secundário sem afetar o ambiente de produção no site principal;

1.1.10.125. Deve permitir a criação de planos de continuidade customizados para execução automatizada de uma sequência de passos para recuperação de desastres.

1.1.10.126. Deve permitir que seja configurado a execução de scripts customizados no plano de continuidade.

1.1.10.127. Permitir o controle da banda de tráfego de rede durante a execução do backup para nuvem.

1.1.10.128. Replicar VMs no local para alta disponibilidade ou off-site para disaster recovery.

1.1.10.129. Suportar a orquestração de failover e failback das máquinas virtuais replicadas.

1.1.10.130. Deverá permitir a restauração do ambiente VMWare em grande escala caso o ambiente VMWare de produção tenha sido comprometido, reduzindo assim o tempo de retorno e disponibilidade do ambiente VMWare.

1.1.10.131. Deverá suportar controle de acesso baseado em função (RBAC) na nuvem.

1.1.10.132. Deverá permitir e estar licenciado o envio de dados desduplicados para a nuvem.

1.1.10.133. Deverá possibilitar a replicação para armazenamento seguro imutável, WORM (Write Once Read Many), com imagens automaticamente prontas para recuperação, ou seja, caso o site primário tenha seus dados comprometidos, deverá ser possível replicar os dados do site secundário para o primário de forma automática, evitando assim erros com operações manuais.

1.1.10.134. Deverá suportar armazenamento seguro imutável, WORM (Write Once Read Many), para evitar que seus dados sejam criptografados, modificados ou excluídos. E todos os dados salvos nessas instâncias deverão ser protegidos com as seguintes medidas de segurança:

1.1.10.135. Deverá garantir a funcionalidade WORM (Write Once Read Many) em todos os tipos de dados existentes no ambiente da CONTRATANTE, incluindo ambiente de servidores físicos, virtuais e nuvem;

1.1.10.136. Deverá garantir a proteção das imagens de backup para que elas sejam somente leitura e não possa ser modificada, corrompida ou criptografada após o backup.

1.1.10.137. Deverá garantir a propriedade da imagem de backup e não ser possível excluir antes da expiração dos dados.

1.1.10.138. Deverá possuir detecção de anomalias próximo a tempo real no site principal de produção à medida que os backups são criados, e através de uso de inteligência artificial para alertar sobre ataques "ransomware" ou outro tipo de ataques cibernéticos, evitando assim que dados comprometidos sejam replicados.

1.1.10.139. Deverá possuir mecanismos de proteção contra ransomware, devendo, mas não se limitando a:

1.1.10.140. Deverá suportar imutabilidade de dados para plataforma que utilizem protocolo S3;

1.1.10.141. Deverá possuir detecção de anomalias nos dados em tempo de execução de backup;

1.1.10.142. Deverá possuir mecanismo de detecção de malwares nos dados armazenados no repositório de backup de maneira automática e manual;

1.1.10.143. Deverá permitir a exclusão de arquivos infectados encontrados no ato de um restore;

1.1.10.144. Detecção e alerta sobre mudanças inesperadas nos dados de backup, com no mínimo os seguintes metadados, atributos ou recursos da tarefa de backup:

1.1.10.144.1. Tamanho da imagem de backup;
1.1.10.144.2. Número de arquivos de backup;
1.1.10.144.3. Dados que são transferidos em KB;
1.1.10.144.4. Taxa de desduplicação;
1.1.10.144.5. Tempo de conclusão do trabalho de backup.

1.1.10.145. Deverá fazer uso de tecnologia de Inteligência Artificial e aprendizagem de máquina para detecção de anomalias;

1.1.10.146. Deverá possuir a capacidade de relatar anomalias como um falso positivo através do cálculo de parâmetro com base nos dados históricos disponíveis após uma determinada frequência oferecendo maior flexibilidade e reduzindo a quantidade de falsos positivos.

1.1.10.147. Qualquer desvio incomum nesses atributos de trabalho de backup deverá ser considerado uma possível anomalia notificando por meio de console WEB e REST-API.

1.1.10.148. Deverá suportar o backup e o restore de diferentes sistemas operacionais tais como:
1.1.10.148.1. Windows (8/10/2012/2012 R2/2016/2019/2022);
1.1.10.148.2. Oracle Linux (7 e 8);
1.1.10.148.3. Red Hat Enterprise Linux (7 e 8);
1.1.10.148.4. Suse Enterprise Server (12 e 15);
1.1.10.148.5. Oracle Solaris (10 e 11);
1.1.10.148.6. AIX (7.1 e 7.2);
1.1.10.148.7. Ubuntu (16, 18 e 20)
1.1.10.148.8. Deverá suportar ambientes virtuais como VMware vSphere (6.7 e superiores) e Hyper-V (2012/2016/2019).

1.1.10.149. Para ambientes com VMware vSphere devrá ser comprovadamente compatível com o VADP (vStorage API for Data Protection) para realizar operações de Backup e Restore de ambientes VMware versão 6.5 e superior;

1.1.10.150. Para ambientes Microsoft Hyper-V, deverá suportar Microsoft Hyper-V Server 2012/R2, Microsoft Hyper-V Server 2016 e Microsoft Hyper-V Server 2019.

1.1.10.151. Deverá suportar VMware vCloud, possuindo integração com vCloud Director API possibilitando backup automático das máquinas virtuais e recuperação completa;

1.1.10.152. Possuir suporte a backup e restore de máquinas virtuais VMware 6.5 ou superior através de vStorage API com as seguintes características:

1.1.10.153. Deverá permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja possível recuperar a imagem completa da máquina virtual Windows e Linux (vmdk), e também arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos vmdk;

1.1.10.154. Deverá suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup;

1.1.10.155. Deverá permitir a identificação de aplicações Microsoft Exchange, SQL e SharePoint que residem r máquinas virtuais, através de integração VADP, permitindo o backup, recuperação integral ou granular dessas aplicações;

1.1.10.156. Deverá permitir a recuperação granular de arquivos/aplicações através da execução de um único backup;

1.1.10.157. Deve permitir o descobrimento automático das máquinas virtuais nos ambientes VMware, com capacidade de realizar filtros avançados com critérios que incluam pelo menos:
1.1.10.157.1. Nome da máquina virtual;
1.1.10.157.2. Sistema Operacional;
1.1.10.157.3. DataStore (Vmware);
1.1.10.157.4. vApp;
1.1.10.157.5. vSAN;
1.1.10.157.6. Tag name;

1.1.10.158. Deve suportar o backup BLIB (Block Level Incremental Backup e Restore) ou FLIB (File Level Incremental Backup e Restore);

1.1.10.159. Deverá possuir a capacidade de balanceamento de carga automática dos backups através de múltiplos backups hosts;

1.1.10.160. Deverá suportar Vmware vSphere 6.5 ou superiores;

1.1.10.161. Deverá permitir restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do seu repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantânea;

1.1.10.162. Prover otimização do backup e recursos (tape / disco), permitindo que somente blocos utilizados sejam copiados no processo de backup;

1.1.10.163. Permitir realizar restauração, através de um único backup, de Máquina virtual completa ou arquivos de dentro da máquina virtual para ambientes Windows e Linux, sem a necessidade de instalação de agentes nas VMs de origem e destino;

1.1.10.164. Possuir a capacidade de restaurar a VM de origem em um ponto no tempo enviando apenas a diferença dos blocos entre a VM de origem e imagem de backup para ambiente VMware através da integração com o VADP;

1.1.10.165. Deverá permitir a visualização, monitoração e recuperação de máquinas virtuais através de plugin integrado ao vCenter ou vSphere 6.5 Web Client ou superior;

1.1.10.166. Deverá possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais;

1.1.10.167. Deverá possuir capacidade de realizar backup de máquinas virtuais em estado online e offline;

1.1.10.168. Deverá possuir a capacidade de movimentação dos dados de backup e restore através de SAN e LAN utilizando os métodos de transporte SAN (LAN-free), NBD e HotAdd;

1.1.10.169. Deverá possuir a capacidade de realizar backup de máquinas virtuais existentes em um vApp;

1.1.10.170. Deverá possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos vmfs ou RDM;

1.1.10.171. Deverá suportar integração com vCloud Director API possibilitando backup automático das máquinas virtuais e recuperação completa;

1.1.10.172. Deverá suportar a recuperação de máquinas virtuais que utilizem identificadores do tipo: hostname, display name, BIOS UUID e instance UUID;

1.1.10.173. Deverá possuir a funcionalidade de restauração instantânea de várias máquinas virtuais do ambiente VMWare simultaneamente a partir de uma imagem de backup, garantindo assim uma rápida recuperação do ambiente em caso de desastre.

1.1.10.174. Deverá ser possível recuperar uma máquina virtual várias vezes de pontos de recuperação diferentes.

1.1.10.175. Possuir suporte a backup e restore de máquinas virtuais Hyper-V, com as seguintes características:

1.1.10.176. Deverá possuir a capacidade de realizar backup On-Host e off-host das máquinas virtuais Windows e Linux;

1.1.10.177. Deverá possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial sem a necessidade de instalação de agentes nas máquinas virtuais;

1.1.10.178. Deverá suportar ambientes configurados com Cluster Shared Volumes;

1.1.10.179. Deverá permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja possível recuperar a imagem completa da máquina virtual Windows e Linux (vhd), e também arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos vhd

1.1.10.180. Deverá possuir a capacidade de recuperação das máquinas virtuais para uma área temporária de disco

1.1.10.181. Deverá suportar Microsoft Hyper-V 2012, 2016 e 2019;

1.1.10.182. Possuir suporte a backup e restore de máquinas virtuais Nutanix AVH, com as seguintes características

1.1.10.183. Deverá possuir recursos do Nutanix AHV integrados à console web para fornecer capacidade de configurar, proteger, recuperar e monitorar os recursos do Nutanix AHV a partir de um navegador da web.

1.1.10.184. Deverá possuir integração com Nutanix AHV através de API, ou seja, sem a necessidade de instalação de agentes.

1.1.10.185. Deverá implementar a proteção de dados do ambiente Nutanix AHV nativo na mesma solução e não sendo permitido uma instalação separada para a proteção dos dados do ambiente Nutanix AHV, ou seja deverá possuir uma instalação única da solução de proteção de dados para os ambientes físicos, virtuais Oracle e Nutanix AHV.

1.1.10.186. Deverá permitir que o administrador configure o acesso do usuário e delegue tarefas, como gerenciamento de ativos AHV, acesso a credenciais, proteção de carga de trabalho, recuperação de VM e recuperação de arquivos e pastas.

1.1.10.187. As credenciais Nutanix AHV deverão ser adicionadas ao banco de dados como credenciais nomeadas. O proprietário pode compartilhar credenciais nomeadas com outros usuários ou administradores para reutilização sem revelar as credenciais reais.

1.1.10.188. Após o cluster AHV for adicionado, deverá ser executar um processo automático de descoberta de recursos e adicionar todas as VMs.

1.1.10.189. Após a execução inicial, o processo de descoberta de recursos deverá ser executado em um intervalo agendado configurável, garantindo assim que todas as VMs adicionadas recentemente sejam incluídas no backup.

1.1.10.190. Deverá permitir executar backup ad hoc fora da programação de backup.

1.1.10.191. Deverá permitir controlar os recursos AHV do Nutanix durante as operações de backup, controlando o número de backups que podem ser executados em um recurso Nutanix AHV.

1.1.10.192. Deverá possuir assistente de recuperação da através de interface java ou web

1.1.10.193. Deverá permitir restaurar todo o AHV VM para o mesmo ou para um cluster AHV diferente.

1.1.10.194. Deverá permitir a restauração de arquivos e pastas individuais de AHV VM protegida para qualquer host de destino. O host de destino pode ser uma máquina virtual hospedada em AHV ou outros hipervisores ou até mesmo uma máquina física

1.1.10.195. Deverá suportar os seguintes bancos de dados, utilizando agente específico:

- **1.1.10.195.1.** Microsoft SQL Server versões 2012, 2014, 2016, 2017 e 2019;
- **1.1.10.195.2.** Oracle/Oracle RAC versões 11g, 12c, 18c, 19c e 21c.
- **1.1.10.195.3.** Microsoft Exchange 2013, 2016 e 2019;
- **1.1.10.195.4.** Microsoft Sharepoint 2013, 2016 e 2019;
- **1.1.10.195.5.** MySQL 5 e 8;
- **1.1.10.195.6.** PostgreSQL 9, 10, 11, 12 e 13;
- **1.1.10.195.7.** MariaDB 10;
- **1.1.10.195.8.** SAP e SAP HANA;
- **1.1.10.195.9.** IBM DB2;
- **1.1.10.195.10.** Microsoft Active Directory.

1.1.10.196. Deverá suportar backup do Oracle Database, incluído arquitetura Oracle RAC, através da integração com RMAN;

1.1.10.197. Deve suportar backup e restore via Agentes Linux para arquiteturas Oracle Real Application Clusters (RAC) e Automatic Storage Management (ASM)

1.1.10.198. Deverá manter a sincronia entre os catálogos de backups do Oracle RMAN e da solução ofertada;

1.1.10.199. Deverá possuir funcionalidade para descoberta automática de instancias Oracle através de consultas periódicas aos clientes de bancos de dados;

1.1.10.200. A funcionalidade de descoberta automática de instancias deverá ser capaz de gerar os scripts RMAN no momento de execução do backup;

1.1.10.201. Deverá possuir funcionalidade de acesso instantâneo para banco de dados Oracle, diretamente repositório de backup;

1.1.10.202. Deverá suportar Apache Hadoop e Apache HBase;

1.1.10.203. Deverá suportar DAG (DataBase Availability Groups) do MS Exchange;

1.1.10.204. Deverá suportar backup do Information Store de Microsoft Exchange, com possibilidade de restore granular, ou seja, de e-mails únicos, itens de calendário e também de caixa postal de algum usuário;

1.1.10.205. Deverá suportar backup do Microsoft Active Directory, com possibilidade de restore granular, ou seja, restauração de todo um diretório, de objetos selecionados e até de atributos individuais;

1.1.10.206. Deverá suportar backup completo do Sharepoint, com possibilidade de recuperação de uma ou mais databases, documentos individuais, sites, subsites, listas e itens/documentos individuais;

1.1.10.207. Deverá permitir o backup e restauração nativamente de aplicativos Kubernetes com no mínimo as seguintes características:

1.1.10.208. Deverá suportar proteção nativa de ambientes Kubernetes integrado com o software de backup.

1.1.10.209. Permitir backup e restauração de aplicativos Kubernetes na forma de namespaces.

1.1.10.210. Configuração do cluster Kubernetes e gerenciamento seguro de credenciais.

1.1.10.211. Descoberta automática e sob demanda de ativos do Kubernetes.

1.1.10.212. Plug-in de serviço de ativos do Kubernetes.

1.1.10.213. RBAC na granularidade do cluster e nível de namespace.

1.1.10.214. Backups baseados em plano de proteção em nível de namespace.
1.1.10.215. Opções de recuperação versáteis, como namespace completo, um recurso personalizado individual ou um volume persistente individual.
1.1.10.216. Gerenciamento do ciclo de vida da imagem com retenção e limpeza personalizáveis.
1.1.10.217. Limitação de recursos por cluster do Kubernetes.
1.1.10.218. Deverá possuir descoberta inteligente e automática de ativos.
1.1.10.219. Deverá permitir executar backups baseados em snapshot sem a utilização de agentes.
1.1.10.220. Deverá possuir controle de fluxo de recursos e recuperação de local alternativo.
1.1.10.221. Deverá prover relatórios gerenciais de backup com no mínimo as seguintes informações:
- **1.1.10.221.1.** Backups com sucesso;
- **1.1.10.221.2.** Backups com falha;
- **1.1.10.221.3.** Volumetria de backup realizado;
- **1.1.10.221.4.** Restore com sucesso;
- **1.1.10.221.5.** Restores com falha;
- **1.1.10.221.6.** Volumetria de restore realizado;
- **1.1.10.221.7.** Clientes de backup configurados;
- **1.1.10.221.8.** Ocupação no destino de backup;
- **1.1.10.221.9.** Licenciamento e capacidade;

1.1.10.222. Possuir interface web para gerenciamento, monitoramento, emissão de alertas, emissão de relatórios sobre operações de backup e restore e emissão de relatórios, com as seguintes características:
1.1.10.223. Relatórios sobre capacidade e tendência de crescimento do ambiente;
1.1.10.224. Se houver múltiplos ambientes de backup, com independência operacional e localizados em diferentes Data Centers, deverá possuir nativamente uma única interface web deverá ser capaz de monitorar e agregar informações de diversos Servidores da Camada de Gerenciamento para emissão dos relatórios;
1.1.10.225. Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente;
1.1.10.226. Deverá permitir exportar relatórios;
1.1.10.227. Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 dias;

1.1.11. ITEM 11 - SOLUÇÃO DE PROTEÇÃO PARA AMBIENTES COLABORATIVOS

1.1.11.1. Deverão ser fornecidas licenças no modelo de subscrição para usuários, incluindo todas as funcionalidades solicitadas para proteção de dados do Microsoft Office 365.
1.1.11.2. Para fins de licenciamento, deverão ser considerados apenas usuários ativos e com licença da Microsoft aplicada.
1.1.11.3. A solução de Proteção de Dados a ser ofertada deve atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças e infraestrutura que forem necessárias para entrega funcional da solução.
1.1.11.4. Deverá ser fornecido proteção para no mínimo 10 GB (dez gigabytes) de armazenamento na origem por licença, independentemente do volume a ser consumido no armazenamento de backup.
1.1.11.5. Deverá ser fornecido backup e recuperação para Exchange Online, OneDrive, SharePoint Online e Teams, bem como log de auditoria do 365.
1.1.11.6. Deverá suportar arquivamento de dados para SharePoint
1.1.11.7. Deverá possibilitar exportar dados para o formato PST.
1.1.11.8. Deverá suportar end-user self-service restore
1.1.11.9. Deverá prover a proteção das cargas de trabalho por meio de conexões seguras.
1.1.11.10. Deverá ser possível definir o escopo e a programação do backup de acordo com as necessidades da CONTRATANTE.
1.1.11.11. Deverá após a implementação permitir que os backups sejam agendados automaticamente.
1.1.11.12. Deverá suportar recuperações completas e granulares em vários níveis.
1.1.11.13. Deverá ser possível recuperar o dado no local, em um local novo ou alternativo, por meio do Microsoft 365 ou para destino externo.
1.1.11.14. Deverá ser possível replicar dados para locais externos ao armazenamento principal, tais como:
1.1.11.15. on-premise para nuvem.
1.1.11.16. nuvem para on-premise.

1.1.11.17. nuvem para outro provedor de nuvem.
1.1.11.18. Deverá prover monitoramento do status e cobertura de backup.
1.1.11.19. Deverá preservar dados para casos de litígio.
1.1.11.20. Deverá ser possível criar e gerenciar casos para litígio e privacidade de dados através de um portal de descoberta eletrônica (eDiscovery).
1.1.11.21. Deverá ser possível pesquisar por metadados, tais como nomes de usuário, arquivos, pastas e datas.
1.1.11.22. Deverá manter os dados seguros com criptografia AES de 256 bits integrada;
1.1.11.23. Deverá prover segurança e com restrições de IPs.
1.1.11.24. Deverá ser possível consultar e relatar o histórico de atividades dos usuários.
1.1.11.25. Deverá ser possível aplicar períodos de retenção imutáveis.
1.1.11.26. Deverá ser possível selecionar regiões de hospedagem em território nacional.
1.1.11.27. Deverá ser possível executar réplicas síncronas de dados para alta disponibilidade.
1.1.11.28. Deverá ser possível executar réplicas em diferentes nuvens, sendo aceitas réplicas assíncronas para estes casos.
1.1.11.29. Deverá prover controle de acesso baseado em função, sendo possível configurar e controlar os acessos de vários tipos de usuários com no mínimo, as seguintes opções:
1.1.11.30. Papéis de acesso pré-definidos.
1.1.11.31. Papéis de acesso customizados.
1.1.11.32. Deverá possuir um SLA do tipo 3, ou seja, 99,9% de tempo de atividade.
1.1.11.33. Deverá ser oferecida no modelo SaaS (Software como serviço) pelo fabricante, não necessitando de nenhuma infraestrutura local ou IaaS (Infraestrutura como serviço) para seu pleno funcionamento.
1.1.11.34. Toda a infraestrutura de hardware, software e prestação de serviço na nuvem deverão ser fornecidos pela CONTRATADA, ou seja, a CONTRATANTE irá contratar o serviço e toda a infraestrutura necessária será de responsabilidade da CONTRATADA.
1.1.11.35. Nos casos de replicações para locais externos (On-premises ou nuvem), a infraestrutura de destino é de responsabilidade da CONTRATANTE.
1.1.11.36. Deverá possuir integração nativa com o software para proteção de dados, provendo console de monitoramento centralizado.
1.1.11.37. Deverá prover até 3 (três) cópias locais de segurança em ambiente Cloud, garantindo a salvaguarda dos dados em casos de falhas de hardware e garantindo a disponibilidade do mesmo.
1.1.11.38. O fabricante da solução de proteção de dados para Microsoft 365 deverá comprovar através de documentações oficiais a segurança física e lógica de seus data centers assim como a garantia da privacidade dos dados.
1.1.11.39. O fabricante da solução de proteção de dados para Microsoft 365 deverá entregar tal proteção na modalidade SaaS (Software como Serviço) e comprovar através de documentações oficiais.
1.1.11.40. Deverá proteger as cargas de trabalho por meio de conexões seguras.
1.1.11.41. Deverá permitir definir o escopo e o agendamento do backup de acordo com as necessidades e políti de retenção da CONTRATANTE.
1.1.11.42. Deverá adicionar os usuários novos nas políticas de backups programados automaticamente.
1.1.11.43. Deverá permitir recuperar o dado no local, em um local novo ou alternativo, através do Microsoft 365, ou para destino externo;
1.1.11.44. Deverá ser possível monitorar e relatar o status e cobertura do backup;
1.1.11.45. Deverá possuir funcionalidade que garanta a segurança dos dados com criptografia AES de 256 bits integrada, fim a fim.
1.1.11.46. Deverá possuir integração do Azure AD ou similar de outras clouds públicas.
1.1.11.47. Deverá possuir a funcionalidade para restringir os IPs, garantindo que somente os IPs cadastrados terão acesso.
1.1.11.48. Deverá possuir logs de auditoria que seja possível consultar e relatar os históricos de atividades de usuários e processos do sistema.
1.1.11.49. Deverá preservar dados para casos de litígio.
1.1.11.50. Deverá ser possível criar e gerenciar casos para litígio e privacidade de dados;
1.1.11.51. Deverá ser possível pesquisar por nomes de usuário, arquivos, pastas e datas;
1.1.11.52. Deverá ser possível aplicar políticas de retenção e garantir que os dados estarão imutáveis;
1.1.11.53. Deverá ser possível selecionar regiões de hospedagem, sendo pelo menos 1 data center no Brasil.

1.1.11.54. Deverá possuir até 3 (três) cópias locais e com réplicas síncronas de dados para alta disponibilidade dos dados;
1.1.11.55. Deverá possui uma console de gerenciamento acessível via web browser.
1.1.11.56. Suportar controle de acesso com "single sign-on" via AD FS 2.0 ou Azure AD ou similar de outras clouds públicas:
1.1.11.57. Suportar duplo fator de autenticação para acesso a console.
1.1.11.58. Deve suportar Single-Tenant para salvaguarda dos dados de backup da Contratante
1.1.11.59. Suportar proteção de dados de, no mínimo, os seguintes itens do Microsoft 365:
- **1.1.11.59.1.** E-mail
- **1.1.11.59.2.** Calendário
- **1.1.11.59.3.** Contatos
- **1.1.11.59.4.** Tarefas
- **1.1.11.59.5.** Notas
- **1.1.11.59.6.** OneDrive
- **1.1.11.59.7.** Arquivos
- **1.1.11.59.8.** Pastas
- **1.1.11.59.9.** Permissões
- **1.1.11.59.10.** SharePoint Online (Qualquer tipo de conteúdo dos sites, incluindo permissões e todos os metadados)
- **1.1.11.59.11.** Teams
- **1.1.11.59.12.** Sites de equipes
- **1.1.11.59.13.** Membros
- **1.1.11.59.14.** Permissões de membros
- **1.1.11.59.15.** Canais
- **1.1.11.59.16.** Postagens
- **1.1.11.59.17.** Arquivos
- **1.1.11.59.18.** Wiki
- **1.1.11.59.19.** Bate-papos individuais e em grupo

1.1.11.60. Realizar a imagem (backup) do ambiente Microsoft 365, no mínimo, de 2 vezes ao dia.
1.1.11.61. Deverá reter as imagens (backup) por todo período de subscrição sem custo adicional.
1.1.11.62. Deverá incluir novos usuários automaticamente, dentro da quantidade de licenças contratadas.
1.1.11.63. Deve suportar operação de recuperação das informações protegidas.
1.1.11.64. Restaurar os dados para no mínimo atender os seguintes níveis:
- **1.1.11.64.1.** Pacote Microsoft 365
- **1.1.11.64.2.** E-mail
- **1.1.11.64.3.** Calendário
- **1.1.11.64.4.** Contatos
- **1.1.11.64.5.** Tarefas
- **1.1.11.64.6.** Notas
- **1.1.11.64.7.** OneDrive
- **1.1.11.64.8.** Arquivos
- **1.1.11.64.9.** Pastas
- **1.1.11.64.10.** Permissões
- **1.1.11.64.11.** SharePoint Online (Qualquer tipo de conteúdo dos sites, incluindo permissões e todos os metadados)
- **1.1.11.64.12.** Teams
- **1.1.11.64.13.** Sites de equipes
- **1.1.11.64.14.** Membros
- **1.1.11.64.15.** Permissões de membros
- **1.1.11.64.16.** Canais
- **1.1.11.64.17.** Postagens
- **1.1.11.64.18.** Arquivos
- **1.1.11.64.19.** wiki
- **1.1.11.64.20.** Bate-papos em grupo

1.1.11.65. Disponibilizar, no mínimo, as seguintes formas de recuperação dos dados:
- **1.1.11.65.1.** Recuperação para o local de origem;
- **1.1.11.65.2.** Novo local ou alternativo, através do M365;
- **1.1.11.65.3.** Fazer download do arquivo.

1.1.11.66. Disponibilizar logs de auditoria para as operações de descoberta legal, auditorias e investigações com pelo menos:
- **1.1.11.66.1.** Administrador - Todas as atividades realizadas por usuários administrativos e privilegiados no portal de administração;

1.1.11.67. Deverá suportar proteção de dados para Google Workspace integrado via Google API. Não serão aceitas soluções que utlizem servidores de proxys como getaway.

1.1.11.68. Deverá suportar proteção de dados para Google Workspace

1.1.11.69. Deve suportar backup e restore granular de folders e mensagens do Gmail.

1.1.11.70. "Deverá suportar o backup e restore dos seguintes tipos de documentos:

1.1.11.71. HTML, HTML (compressed), Plain text, Rich text, Open Office doc, PDF, Microsoft Word document, EPUB, Open Office sheet, PDF, CSV (first sheet only), Sheet only, HTML (compressed), JPEG, PNG, SVG, Microsoft PowerPoint, Open Office presentation, PDF, Plain, text, JSON."

1.1.11.72. Deverá suportar arquitetura de Backup como Serviço (BaaS).

1.1.11.73. Deverá suportar funcionalidade de criptografia durante todo o processo de proteção dos dados.

1.1.11.74. A solução deverá suportar salvaguardar os dados em diferentes regiões e domínios na Cloud.

1.1.11.75. Deverá suportar a proteção dos metadados.

1.1.11.76. Deverá suportar restore granular para local de origem dos dados e demais destinos alternativos.

1.1.11.77. Deve suportar restore granular de folders, tabelas e anexos e arquivos compartilhados via Google Drive.

1.1.11.78. Suportar restore de Google Docs, Sheets, Slides, Drawings, and Scripts.

1.1.11.79. Deverá suportar criação de políticas de backup e restore com permissões para Clouds em diferentes regiões.

1.1.11.80. Suportar auditoria

1.1.11.81. Suportar MFA2 - Múltiplo fator de autenticação.

1.1.11.82. Suportar role-based access control (RBAC).

1.1.11.83. Deve suportar retenções ilimitadas de backup.

1.1.11.84. Deve suportar imutabilidade dos dados

1.1.11.85. Suportar permissionamento de regras por endereçamento IP.

1.1.11.86. Suportar Point-in-time restore.

1.1.11.87. Suportar criptografia fim a fim de no mínimo 256 Bits.

1.1.12. ITEM 12 – SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – MONITORAMENTO E MITIGAÇÃO DE RISCOS ÀS IDENTIDADES DA TI

1.1.12.1. Características Gerais da Solução:

1.1.12.1.1. A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.

1.1.12.1.2. Apoiando os requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente.

1.1.12.1.3. Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;

1.1.12.1.4. Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e uso de credenciais por ela gerenciadas.

1.1.12.1.5. Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos os comportamentos anormais de, pelo menos, 50 usuários simultâneos acessando todos sistemas-alvo do ambiente tecnológico, dentre eles servidores Linux/Unix, Windows, controladores de domínio Microsoft Active Directory, estações de trabalho Windows e demais ativos de rede e sistemas computacionais diversos.

1.1.12.1.6. A solução deverá ser entregue com acesso remoto seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a necessidade de instalação e uso de clientes e VPN nos dispositivos dos usuários remotos por todo período de assinatura contratado.

1.1.12.1.7. A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:

1.1.12.1.8. Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coordenadas GPS e banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware).

1.1.12.1.9. Autenticação autoajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento.

1.1.12.1.10. Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de logon, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo.

1.1.12.1.11. Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação.

1.1.12.1.12. Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados.

1.1.12.1.13. Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: VMWare e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc; Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP, Office 365.

1.1.12.2. Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:

1.1.12.2.1. A solução deve conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH", disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio

de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

1.1.12.2.2. A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.

1.1.12.2.3. Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;

1.1.12.2.4. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;

1.1.12.2.5. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;

1.1.12.2.6. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;

1.1.12.2.7. Deve proteger as senhas de credenciais administrativas locais de todas as estações de trabalho Windows no repositório central seguro de credenciais, permitindo a aplicação de políticas granulares de rotações e trocas automáticas das senhas, trilha de auditoria dos acessos às mesmas, mitigando situações de roubo, perda e exploração de credenciais.

1.1.12.2.8. Quando as estações de trabalho não puderem estar conectadas de forma permanente repositório central de credenciais, deve aplicar, de forma autônoma, políticas de rotação de credenciais locais até a sincronização das mesmas definidas no repositório central da solução.

1.1.12.2.9. Possuir funcionalidade de "AD Bridge" para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;

1.1.12.2.10. Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;

1.1.12.2.11. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;

1.1.12.2.12. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões do usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; suporta métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e mail;

1.1.12.2.13. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;

1.1.12.2.14. Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;

1.1.12.3. Análise comportamental e mitigações de risco no ambiente crítico para Identidades Privilegiadas:

1.1.12.3.1. A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.

1.1.12.3.2. Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como nova autenticação, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:

1.1.12.4. Acessos a solução:

1.1.12.4.1. Durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental);

1.1.12.4.2. Durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental);

1.1.12.4.3. Através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental);

1.1.12.5. Acessos gerais:

1.1.12.5.1. Usuários incomuns logando de uma máquina de origem conhecida;

1.1.12.5.2. Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução).

1.1.12.6. Máquinas:

1.1.12.6.1. Acessadas a partir de endereços IP incomuns;

1.1.12.6.2. Acessadas durante horários irregulares, de acordo com seu padrão de utilização;

1.1.12.6.3. Incomuns originando acessos.

1.1.12.7. Credenciais e Contas:

1.1.12.7.1. Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador,

1.1.12.7.2. Deve permitir a configuração de eventos críticos a serem reportados automaticamente baseados em comandos Linux, comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado;

1.1.12.8. Arquitetura e Segurança da Solução

1.1.12.8.1. A solução deve ser entregue no formato SaaS, com uma disponibilidade contratual mínima de 99.5% por ano, comprovado por documentos oficiais do fabricante da solução

1.1.12.8.2. O fabricante da solução deve possuir certificações para garantir a segurança e a continuidade operacional do modelo SaaS com, pelo menos, as certificações SOC2 Type 2 e ISO27001, relevantes ao ambiente do serviço prestado. Tais certificações devem ser realizadas por uma instituição externa acreditada a realizar tal auditoria.

1.1.12.8.3. A solução deve suportar, no mínimo, 25 conectores (componente de conexão entre o datacenter e o serviço SaaS) e 50 JumpServers

1.1.12.8.4. A solução não deve necessitar de regras de firewall INBOUND, ou seja, não deve necessitar de abertura de portas de entrada em nosso ambiente

1.1.12.9. A instalação de componentes locais deve ser suportada em ambientes On-Premises, AWS, Azure e GCP, no mínimo.

1.1.12.9.1. A solução deve permitir o acesso offline às credenciais privilegiadas eleitas como emergenciais por usuários autorizados

1.1.12.9.2. Deve ser fornecido um ambiente de homologação SaaS da solução, com as mesmas características do objeto contratado

1.1.13. ITEM 13 – SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA SERVIDORES WINDOWS E LINUX/UNIX

1.1.13.1. A solução deverá garantir a segurança para identidades e acessos para servidores com sistemas operacionais Microsoft Windows e Linux.

1.1.13.2. Requisitos mínimos aplicados a Servidores Windows:

1.1.13.2.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.1.13.2.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;

1.1.13.2.3. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;

1.1.13.2.4. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;

1.1.13.2.5. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

1.1.13.2.6. Suportar, no mínimo, os seguintes sistemas operacionais:

1.1.13.2.6.1. Windows Server 2012/2012 R2;

1.1.13.2.6.2. Windows Server 2016;

1.1.13.2.6.3. Windows Server 2019;

1.1.13.2.6.4. Windows Server 2022;

1.1.13.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

1.1.13.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos diretamente no ativo;

1.1.13.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo.;

1.1.13.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

1.1.13.2.11. Permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM.

1.1.13.2.12. Permitir a verificação do hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante para objetos reutilizáveis da solução.

1.1.13.2.13. Suportar ao nome exato da aplicação / arquivo / script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

1.1.13.2.14. Utilizar eventos reportados na interface da solução para criação de novas políticas ou incluí-los em políticas existentes;

1.1.13.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

1.1.13.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da console de gerência;

1.1.13.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

1.1.13.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;

1.1.13.2.19. Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras individualmente ou em grupos;

1.1.13.2.20. Realizar varreduras utilizando as funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes;

1.1.13.2.21. Verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou mecanismos de controle de ameaças (VirusTotal.com ou similares);

1.1.13.2.22. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo.

1.1.13.2.23. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line.

1.1.13.2.24. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP.

1.1.13.2.25. Oferecer monitoramento ou detecção quanto a tentativas de roubo de credenciais.

1.1.13.2.26. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução.

1.1.13.2.27. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;

1.1.13.2.28. Permitir criar uma whitelist para execução de aplicativos confiáveis, onde qualquer outra aplicação fora desta lista automaticamente seja bloqueada;

1.1.13.2.29. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;

1.1.13.2.30. Suportar a guarda de políticas de hosts que não fazem parte do Active Directory;

1.1.13.2.31. Possuir cache de políticas aplicadas no endpoint, permitindo a segurança dos endpoints, ainda que ele não esteja conectado à rede corporativa;

1.1.13.2.32. Permitir que mensagens customizadas sejam apresentadas antes que uma aplicação seja executada ou bloqueada;

1.1.13.2.33. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;

1.1.13.2.34. Deve possuir capacidade de gerar relatórios de aplicações e eventos de usuários inclusos na solução;

1.1.13.2.35. Realizar varredura e inventário de aplicações instaladas no sistema operacional;

1.1.13.3. Requisitos mínimos aplicados Servidores Linux:

1.1.13.3.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.1.13.3.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino fazendo uso de agente instalado no sistema ou método análogo;

1.1.13.3.3. Suportar, no mínimo, os seguintes sistemas operacionais:

1.1.13.3.3.1. Debian 9

1.1.13.3.3.2. Redhat Linux 7.x (64-bit);

1.1.13.3.3.3. Redhat Linux 8.x (64-bit).

1.1.13.3.4. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos;

1.1.13.3.5. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular;

1.1.13.3.6. Realizar o controle mediante interceptação do comando antes que ele seja executado;

1.1.13.3.7. Permitir a liberação de comandos privilegiados a usuários comuns;

1.1.13.3.8. Permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro digital;

1.1.13.3.9. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory;

1.1.13.3.10. Permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;

1.1.13.3.11. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;

1.1.13.3.12. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);

1.1.13.3.13. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;

1.1.13.3.14. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;

1.1.13.3.15. Oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;

1.1.13.3.16. Monitorar e exibir acessos e atividades realizadas no próprio sistema;

1.1.13.3.17. Possibilitar mapear e coletar atividades regulares de usuários através do modo observação agregando e exportando os resultados para um perfil;

1.1.13.3.18. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos ou bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;

1.1.13.3.19. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas.

1.1.14. ITEM 14 – SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA ESTAÇÕES

1.1.14.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.1.14.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;

1.1.14.3. Realizar varredura e inventário de aplicações instaladas na estação de trabalho.

1.1.14.4. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente na estação de trabalho de destino (sem ser através do Repositório Seguro), fazendo uso das funcionalidades instaladas no sistema operacional;

1.1.14.5. Oferecer opção de execução de aplicações com privilégios em modo explícito e transparente (sem avisos);

1.1.14.6. Oferecer opção de execução monitorada de aplicações em modo explícito e transparente (sem avisos);

1.1.14.7. Oferecer opção de execução com restrições de aplicações em modo explícito e transparente (sem avisos);

1.1.14.8. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;

1.1.14.9. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

1.1.14.10. Suportar pelo menos as seguintes versões de estações de trabalho:

1.1.14.10.1. Windows 10 x32 & x64;

1.1.14.10.2. Windows 11 x64;

1.1.14.11. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via Repositório Seguro ou diretamente no ativo;

1.1.14.12. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo;

1.1.14.13. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

1.1.14.14. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

1.1.14.15. Permitir a criação de objetos reutilizáveis que possam conter no mínimo os seguintes tipos: arquivos executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX e objetos COM;

1.1.14.16. Implementar a verificação de hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

1.1.14.17. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

1.1.14.18. Utilizar eventos reportados na interface da ferramenta para novas políticas ou incluí-los em políticas existentes;

1.1.14.19. Permitir agrupamento de características e aplicações para fácil seleção e inclusão em políticas de segurança;

1.1.14.20. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;

1.1.14.21. Disponibilizar modo de observação, em que não há bloqueios, mas há o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

1.1.14.22. Monitorar e exibir acessos e atividades realizadas na própria solução;

1.1.15. ITEM 15 – SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – AUTENTICAÇÃO MULTI-FATOR COM INTELIGÊNCIA DE AMEAÇAS

1.1.15.1. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:

1.1.15.1.1. Aplicações Web integradas nas funções de Logon único adaptativo para usuários - Single sign-on.

1.1.15.1.2. Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML.

1.1.15.1.3. Qualquer disposito ou sistema operacional que suporte RADIUS.

1.1.15.1.4. Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services.

1.1.15.1.5. Sob demanda utilizando o protocolo Oauth e REST APIs.

1.1.15.1.6. Para realizar o autosserviço de reset de senha ou desbloqueio de usuário.

1.1.15.2. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:

1.1.15.2.1. Usuário e senha dos diretórios suportados na solução.

1.1.15.2.2. Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para:

1.1.15.2.3. Biometria do tipo FaceID.

1.1.15.2.4. Biometria através do leitor de digital.

1.1.15.2.5. Smartphone push (Notificação para aprovar ou recusar uma autenticação).

1.1.15.2.6. Geolocalização abanco de dados de IPs.

1.1.15.2.7. Suporte a tokens OATH OTP.

1.1.15.2.8. Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel.

1.1.15.2.9. Ligação telefônica requisitando um PIN previamente configurado.

1.1.15.2.10. Mensagem de texto via SMS oferecendo o código para entrada manual e também uma URL única presente na mensagem de texto que ofereça a opção de aprovar ou recusar a autenticação sem a necessidade de digitar o código manualmente.

1.1.15.2.11. Confirmação de código via email.

1.1.15.2.12. Clientes do tipo OATH OTP (exemplo, Google Authenticator).

1.1.15.3. Autenticadores que suportem FIDO2 / U2F, minimamente suportando:

1.1.15.3.1. Windows Hello.

1.1.15.3.2. Yubikey.

1.1.15.3.3. Google Titan Key

1.1.15.3.4. MacOS TouchID.

1.1.15.3.5. Perguntas e respostas previamente configuradas.

1.1.15.4. Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal web da solução.

1.1.15.5. Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através de REST APIs oferecidas pela solução.

1.1.15.6. A solução deve possuir SDK (Software Development Kits) para aplicações mobile com suporte para as plataformas IOS e Android, para a Kotlin e Swift respectivamente. Os SDKs devem suportar a integração facilitada das funcionalidades de autenticação via notificações (Aprovar ou Negar), leitura de códigos QR para autenticação em páginas web como também com as funcionalidade de biometria nativas destes sistemas operacionais. Estes SDKs não devem ter um custo adicional e devem ter seu código aberto para a comunidade desenvolvedora.

1.1.15.7. Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:

1.1.15.7.1. Endereçamento IP.

1.1.15.7.2. Dia da Semana.

1.1.15.7.3. Datas específicas.

1.1.15.7.4. Janelas de tempo entre duas datas.

1.1.15.7.5. Janelas de tempo entre horários (exemplo, horário comercial).

1.1.15.7.6. Tipo do Sistema Operacional.

1.1.15.7.7. Tipo do Browser.

1.1.15.7.8. Perfis configurados na solução.

1.1.15.7.9. País que está sendo realizado o acesso.

1.1.15.7.10. Se é um dispositivo gerenciado.

1.1.15.7.11. Autenticação via certificado.

1.1.15.7.12. Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.

1.1.15.8. A solução deve ter a capacidade de verificar antes de realizar um login em uma aplicação se o endpoint gerenciado está em conformidade com a solução de gerenciamento de endpoint (Unified Endpoint Management - UEM), devendo suportar minimamente:

1.1.15.8.1. Microsoft Intune

1.1.15.8.2. vmware Workspace One

1.1.15.8.3. JAMF

1.1.15.9. A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelos usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo.

1.1.15.10. O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:

1.1.15.10.1. Conjunto de aplicações.

1.1.15.10.2. Uma única aplicação.

1.1.15.10.3. Regras para o autosserviço de reset de senha e desbloqueio de usuário.

1.1.15.10.4. Portal do Administrador.

1.1.15.10.5. Portal do Usuário.

1.1.15.11. A solução deve prover um portal WEB para o usuário final com as seguintes características:

1.1.15.11.1. Permitir o usuário realizar o auto registro de seus fatores de autenticação, tais como, perguntas e respostas, FIDO2 tokens, OATH OTP, definir PIN para chamada telefônica, TouchID, FaceID, Windows Hello, dentre outros.

1.1.15.11.2. Permitir o usuário redirecionar autenticação multi fator para outros usuários (desde que permitido).

1.1.15.11.3. Permitir os usuários gerenciarem seus dispositivos registrados, minimamente:

1.1.15.11.4. Smartphones Android e IOS.

1.1.15.12. Para cada dispositivo registrado, os usuários devem ter as seguintes capacidades de gestão:

1.1.15.12.1. Realizar o auto registro de novos dispositivos móveis.

1.1.15.13. A solução deve prover um aplicativo móvel para Android e IOS com as seguintes características:

1.1.15.13.1. Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO já integrado com os navegadores instalados nos dispositivos móvel.

1.1.15.13.2. Prover login através do scan de QRcode no portal web permitindo SSO sem identificação de usuário e senha.

1.1.15.13.3. Configurar OATH OTP adicionais provenientes de outras soluções.

1.1.15.13.4. Verificar dispositivos registrados (dispositivos móveis e sistemas operacionais).

1.1.15.13.5. Integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autenticação biométrica durante login nas aplicações.

1.1.15.13.6. Reportar coordenadas GPS para os sistemas que utilizam geolocalização.

1.1.15.13.7. Detectar ROOT em dispositivos Android e Jailbreak em dispositivos IOS com a finalidade de detectar atividades maliciosas e como consequência o aplicativo é desabilitado para uso

1.1.15.14. O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente:

1.1.15.14.1. Data e Hora.

1.1.15.14.2. Cidade / Geolocalização do acesso

1.1.15.14.3. Aplicação sendo acessada.

1.1.15.15. A solução deve possuir a capacidade de realizar o login sem a utilização da senha (passwordless) realizando o scan de QR code gerado na tela de login do portal de aplicação através do aplicativo móvel do fabricante, sem a necessidade inclusive de digitar o usuário a ser logado na aplicação. Deve adicionalmente ter a opção de forçar a utilização de biometria oferecida pelo smartphone / telefone celular.

1.1.15.16. A solução deve possuir um aplicativo para Windows e MacOs com suporte a multifator de autenticação do tipo OTP (one time password) do próprio fabricante da solução de multifator. Este aplicativo dará suporte para casos em que não será possível o uso de um telefone celular / smartphone.

1.1.15.17. Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

1.1.15.18. Realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;

1.1.15.19. Verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou mecanismos de controle de ameaças (VirusTotal.com ou similares);

1.1.15.20. Permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;

1.1.15.21. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional;

1.1.15.22. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

1.1.15.23. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

1.1.15.24. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo *sandbox*.

1.1.15.25. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados.

1.1.15.26. Permitir a salvaguarda das contas privilegiadas em um único repositório seguro.

1.1.15.27. A solução deve fornecer proteção de grupos de privilégios, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users;

1.1.15.28. Solução deve automaticamente permitir os aplicativos de lista branca implantados por ferramentas de implantação de software por administradores confiáveis, incluindo o SCCM (Microsoft System Center Configuration Manager)

1.1.15.29. A solução deve permitir criar uma lista de aplicativos permitidos (allow list), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista seja bloqueada automaticamente.

1.1.15.30. Permitir criar uma lista branca (whitelist) de aplicativos, onde é configurado todos os aplicativos que podem ser executados, onde qualquer outra aplicação fora desta lista, seja automaticamente seja bloqueada;

1.1.15.31. A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados para cálculo de risco.

1.1.15.32. A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:

1.1.15.32.1. Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando "viagens impossíveis", e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam.

1.1.15.32.2. Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.

1.1.15.32.3. Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.

1.1.15.32.4. Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.

1.1.15.32.5. Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual

1.1.15.32.6. Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual

1.1.15.33. O cálculo do risco pelo motor de aprendizado de máquina não utilize somente um atributo fora da normalidade reconhecida anteriormente pelo mesmo, mas sim em uma única autenticação calcule o risco baseado em todos os atributos citados acima e suas anormalidades em uma única autenticação. Exemplo, uma identidade tem por costume realizar sua autenticação as 9,10 e 11 da manhã, nas aplicações A e B, nas segundas-feiras e quintas-feiras, utilizando um dispositivo Android, das cidades de Brasília e São Paulo. Em futuro login acaba realizando a autenticação as 14 horas (fora do seu horário regular), na aplicação A, em um sábado (não é um dia da semana usual para esta identidade), de um dispositivo IOS (também não usual), da cidade de Brasília. O motor de aprendizado de máquina deve ter a capacidade de reconhecer estes três desvios de comportamento e retornar um risco calculado (alto, médio, baixo ou sem risco) referente a mesma.

1.1.15.34. A solução deverá prover múltiplo fator de autenticação para casos de uso com capacidade de interpretação de risco adaptativo baseados em algoritmos de aprendizado de máquina e reconhecimento de comportamentos temporais para cada identidade (dias da semana e horários), o mesmo calculado antes da autenticação para tomada de ações antes da materialização da autenticação.

1.1.15.35. Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:

1.1.15.35.1. Sem risco

1.1.15.35.2. Risco Baixo

1.1.15.35.3. Risco Médio

1.1.15.35.4. Risco Alto

1.1.15.36. Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;

1.1.15.37. O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:

1.1.15.37.1. Requisitar múltiplos fatores de autenticação de forma dinâmica.

1.1.15.37.2. Permitir o login sem o uso de múltiplos fatores.

1.1.15.37.3. Negar a autenticação.

1.1.15.38. Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que o influenciaram, além da exploração dos eventos capturados e seus atributos.

1.1.15.39. Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis

1.1.15.40. Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV adicionalmente gravar as visualizações na solução para consultas posteriores.

1.1.15.41. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado como, por exemplo, Palo Alto Cloud.

1.1.15.42. Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo:

1.1.15.42.1. E-mail com conteúdo do alerta.

1.1.15.42.2. Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack.

1.1.15.43. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:

1.1.15.43.1. Utilização do Motor de Análise do Comportamento dos Usuários.

1.1.15.43.2. Comportamento dos usuários na utilização das aplicações.

1.1.15.43.3. Visão sobre a segurança das aplicações.

1.1.15.43.4. Mapa com a geolocalização das autenticações.

1.1.15.43.5. Visão sobre o comportamento dos Endpoints (Mobile e Computadores).

1.1.15.43.6. Visão sobre o comportamento das Identidades.

1.1.15.44. A solução deve permitir a configuração de dashboards personalizados.

1.1.15.45. Deve permitir o compartilhamento dos dashboards com outros usuários.

1.1.16. ITEM 16 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM - GERENCIAMENTO DE CREDENCIAIS DAS IDENTIDADES DO USUÁRIO FINAL

1.1.16.1. A solução deve prover extensão no Browser para capturar aplicações Web que utilizam formulário com usuário e senha e realizar o autopreenchimento do login e senha de forma automatizada. Estas informações devem ser guardadas de forma segura na solução para autopreenchimento nos futuros logins nestas aplicações.

1.1.16.2. A solução deve prover uma extensão de browser avançada somente para administradores da solução, com a finalidade de realizar o mapeamento dos campos dos formulários (em geral login e senha) para que depois de mapeados os administrados possam incluir como uma aplicação Web para SSO no catálogo geral, permitindo o SSO de aplicações que não suportam protocolos mais modernos como SAML , Oauth e OIDC.

1.1.16.3. Permitir o usuário de negócio/comum armazenar credenciais Web que não estão conectadas ao IDP / SSO, ou seja, diferentes da das credenciais dos mesmos em um cofre pessoal na nuvem da solução e integrando com algum cofre on-premises de soluções PAM de mercado.

1.1.16.4. Permitir o SSO das credenciais não conectadas ao IDP, removendo as credenciais do cofre em nuvem ou on-premises e injetando as mesmas no formulário de login dessas aplicações web, facilitando a experiência de Login e mantendo um armazenamento seguro destas credenciais de negócio, estas credenciais nunca devem ser armazenadas ou com cache local no dispositivo do usuário final. A solução deve sempre consultar o cofre em nuvem ou on-premises no momento da utilização da credencial.

1.1.16.5. Permitir o usuário de negócio/comum armazenar em cofre em nuvem ou on-premises não somente de credenciais de aplicações web mas também credenciais de aplicações não web, tais como, SAP GUI, Emuladores de terminais etc.

1.1.16.6. Permitir o usuário de negócio/comum compartilhar de forma segura credenciais web, não web e notas seguras com parceiros de trabalho. Durante o compartilhamento o dono da credencial poderá definir uma faixa de tempo que ficará disponível a credencial e se o usuário que receberá acesso poderá visualizar ou não e editar a credencial.

1.1.16.7. Suportar o armazenamento seguro em cofre em nuvem ou on-premises de notas seguras, tais como, senhas de wifi, números de carões de crédito, dentro outras informações que devem ter um armazenamento seguro.

1.1.16.8. Permitir o usuário de negócio/comum que durante o login em uma aplicação web seja detectado o formulário de login e oferecer de forma automatizada a possibilidade de armazenar esta credencial em seu cofre pessoal, além de gravar a automação de login desta aplicação com a finalidade de facilitar a entrada na mesma nos subsequentes logins, sem a necessidade de digitar suas credenciais novamente.

1.1.16.9. Permitir o administrador criar listas não autorizadas com endereços de websites, onde não seja oferecido para seu usuário comum / negócio a possibilidade de embarcar credenciais destes sites listados na mesma.

1.1.16.10. Permitir a transferência automatizada de custódia de credenciais para gerentes imediatos ou identidades configuradas pelo administrador de credenciais armazenadas e compartilhadas por usuário de negócio / comum, caso o mesmo seja desligado da empresa.

1.1.16.11. Todo o fluxo de transmissão das credenciais de negócio armazenadas em nuvem ou em cofre on-premises deve ser criptografado fim-a-fim (end-to-end) com a finalidade de manter a confidencialidade destas credenciais.

1.1.16.12. No momento do cadastro de uma credencial de negócio a solução via extensão do navegador deve sugerir senhas fortes baseadas em complexidade / entropia configuradas pelo usuário final.

1.1.16.13. A extensão de navegador da solução deve suportar minimamente, Microsoft Edge, Google Chrome e Firefox.

1.1.16.14. Permitir o administrador da solução configurar via perfis na solução quem poderá utilizar credenciais compartilhadas, por exemplo, redes sociais, sites de compras, dentre outros. Além de permitir o uso da credencial compartilhada toda a inteligência de automação de login (ingestão da credencial no formulário web de maneira automatizada) também deve ser compartilhado, desta forma o usuário final não necessita visualizar a credencial.

1.1.16.15. A solução deve permitir gerar relatórios detalhados de usuários que utilizaram as credenciais. compartilhamentos de credenciais, visualizações. Com minimamente as seguintes informações, que utilizou, quando, qual credencial, com quem foi compartilhada e IP.

1.1.16.16. Deve possuir um aplicativo móvel para Android e IOS para armazenar credenciais de negócio de usuários finais em seu cofre pessoal, sendo estas credenciais acessíveis pelo aplicativo móvel, interface web e extensão do browser e totalmente sincronizadas independente de qual interface está sendo utilizada para acesso.

1.1.16.17. Quando usuário acessar um website e caso o mesmo possua uma credencial em seu cofre pessoal a extensão do navegador deve detectar e indicar no campo de login da aplicação de forma visual que o mesmo pode utilizar uma credencial armazenada em seu cofre pessoal. Nesta indicação visual no campo de login o usuário pode interagir com a mesma e selecionar a credencial a ser utilizada.

1.1.16.18. Deve ter a capacidade de importar credenciais de outros gerenciadores de senhas pessoais, minimamente suportando, LastPass, Keepass, Dashlane e Google.

1.1.17. ITEM 17 – PLATAFORMA DE REDE DE DISTRIBUIÇÃO DE CONTEÚDO – CDN

1.1.17.1. Deverá ser fornecida subscrição com vigência de 12 (doze) meses dos serviços descritos abaixo;

1.1.17.2. Os serviços a serem contratados devem ser providos mediante uma CDN não intrusiva, ou seja, sem que haja necessidade da contratada instalar equipamentos na CONTRATANTE.

1.1.17.3. Deve estar disponível mediante apontamento do DNS da CONTRATANTE utilizando CNAMES.

1.1.17.4. Os serviços contratados deverão prover a infraestrutura de uma CDN com uma liberalidade de acess medidos em volume de tráfego.

1.1.17.5. Deverá fornecer acesso ao console de gerenciamento de rede de entrega de conteúdo e medidas de segurança pela Internet.

1.1.17.6. Deverá fornecer o gerenciamento de vários usuários com funções e diferentes níveis de permissões de gerenciamento e usuários somente leitura (Somente leitura)

1.1.17.7. A liberalidade de tráfego a ser fornecido mensalmente é de até 5 TB (Terabytes).

1.1.17.8. Deverá prover serviço adicionado de bloqueio de acessos visando evitar que tentativas de ataque sejam contabilizados (tais como DDoS), consumindo franquias contratadas pela CONTRATANTE.

1.1.17.9. Deverá ser provido serviço adicionado de replicação do DNS da CONTRATANTE, visando evitar que ataques ao servidor de nomes da CONTRATANTE impeçam a replicação de conteúdos para a CDN.

1.1.17.10. Deverá ser provido serviço adicional de proteção contra ataques, de forma a proteger os equipamentos servidores da CONTRATANTE, fonte das informações que serão replicadas pela rede de distribuição de conteúdos.

1.1.17.11. Deverá ser descentralizada, sem ponto único de falha, contendo, pelo menos, 180 (cento e oitenta) pontos de presença no mundo, com pelo menos 5 (cinco) no Brasil e 2 (dois) estados da federação distintos, para entrega de conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) em todos os pontos da rede.

1.1.17.12. Deverá possuir cobertura automática para usar os protocolos TLS 1.3, HTTP/2 e Brotli.

1.1.17.13. Deverá ter pontos de presença no Exterior, de modo a atender serviços de infraestrutura de tecnologia em escala global, no mínimo em 70 países, de maneira a suportar qualquer interrupção de serviço em território nacional, através do transbordo de carga de trabalho para outras regiões geográficas. Devendo a mesma obter uma capacidade de mitigação superior a 18 Tbps.

1.1.17.14. Deverá possuir pelo menos três das certificações abaixo (emitidas no Brasil ou no Exterior) e a comprovação das certificações poderá ser feita através de informações disponibilizadas no site do fabricante da solução ou por meio digital, que deverá ser apresentada juntamente com a proposta comercial:

1.1.17.14.1. SOC 2 Tipo 2

1.1.17.14.2. PCI DSS 3.2.1

1.1.17.14.3. ISO/IEC 27001:2013

1.1.17.14.4. ISO 27002:2013

1.1.17.14.5. NIST 800-53 (FedRAMP)

1.1.17.15. Deverá possuir regras de limite de taxa ou com períodos amostrais de 1 (um) segundo a 1 (uma) hora com critérios configuráveis.

1.1.17.16. Deverá possuir a capacidade de detecção e bloqueio de ataques de negação de serviço com recursos de entregar o tráfego legítimo inspecionado pela rede de entrega de conteúdo e descartar tráfego ilegítimo, com detecção automática e negação de ataques de Camada 7, descobrindo e protegendo automaticamente alterações bruscas no tráfego da Camada 7 (POST Floods e DNS-based A acks).

1.1.17.17. Deverá possuir capacidade de exportação de logs e integração com ferramentas de coleta de eventos (SIEM).

1.1.17.18. Deverá possuir armazenamentos em linha (na console do fabricante) de log de auditoria por no mínimo 45 (quarenta e cinco) dias.

1.1.17.19. Deverá possuir capacidade de definição e configuração de vários níveis de segurança, com a capacidade do cliente aumentar o nível de segurança a qualquer momento.

1.1.17.20. Deverá fornecer através do serviço de rede de entrega de conteúdo de firewall de aplicações web (WAF) em execução em tempo real, sem custo adicional. Este WAF deve incluir ao menos as regras de segurança para as 10 (dez) principais vulnerabilidades identificadas pelo Open Web Application Security Project (OWASP).

1.1.17.21. Deverá possuir inteligência para identificar novas ameaças, que devem ser estendidas automaticamente (Base de Reputação IP) na rede de entrega de conteúdo, bem como a capacidade de bloquear ameaças maliciosas conhecidas.

1.1.17.22. Deverá oferecer mitigação contra ataques DDoS de qualquer tipo e capacidade de mitigação de 15 Tbps ou superior, sem custos adicionais para tráfego interceptado.

1.1.17.23. Deverá possuir a capacidade de enviar logs para o push de log de forma configurável com intervalos de 5 (cinco) minutos ou menos .

1.1.17.24. Deverá permitir a personalização de páginas da Web para a implantação de mensagens de aviso e erro.

1.1.17.25. Deverá possuir a proteção de conteúdo, como texto e imagens contra invasores do tipo scrapers.

1.1.17.26. Deverá permitir a criação de regras de segurança personalizadas para os vários sites publicados nos domínios do CONTRATANTE. Essas regras devem permitir bloqueio automático ou manual com as seguintes opções: Ação de estudo (gerar logs), bloqueio, desafio e desafio Javascript por Região (Países e continentes), IP, blocos de IPs, ASN e Agentes de Usuário.

1.1.17.27. Deverá possuir um algoritmo de roteamento dinâmico que caso algum data center fique indisponível o tráfego seja redirecionado sem afetar o desempenho dos serviços e sem acréscimo de latência.

1.1.17.28. Deverá garantir um SLA de 100% de disponibilidade para o serviço prestado divulgado oficialmente no website do fabricante com política de ressarcimento em casos de indisponibilidade. (justificativa, para que evite o desentendimento ao longo do serviço entre cliente, provedor local e fabricante).

1.1.17.29. A contabilização do consumo deve ser reiniciada novamente do zero em todo dia 1 (um) de cada mês.

1.1.17.30. Deverá fazer uso de algoritmos para determinar qual servidor da rede dinâmica possui melhores condições de entrega, utilizando métodos para o redirecionamento do usuário, desde servidores de aplicações, até o redirecionamento no nível de Servidor de Domínio de Nomes (Domain Name Servers, DNS).

1.1.17.31. Deverá obter um modo automático de verificação das conexões dos servidores de origem, a cada 10 (dez) minutos ou menos.

1.1.17.32. Deverá ter a opção de reconstrução de páginas caso haja problemas com a disponibilidade do servidor de origem, devendo ao menos entregar os conteúdos armazenados na rede de CDN.

1.1.17.33. Deverá fornecer pelo menos 2 IPs IPV4 e 2 IPs IPV6 na troca do DNS autoritativo.

1.1.17.34. Deverá permitir o gerenciamento de um número ilimitado de registros DNS, com os seguintes tipos: A, AAAA, CNAME, MX, TXT, SPF, TLSA, NAPTR, HTTPS, CERT, NS, SRV, DS, LOC e CAA.

1.1.17.35. Deverá através do DNSSEC no qual o tráfego é encaminhado com segurança para os servidores corretos, para que não haja possibilidade de que a comunicação seja interceptada.

1.1.17.36. Deverá realizar a análise do serviço DNS considerando no mínimo os seguintes:

1.1.17.37. Dados históricos de consultas feitas ao DNS com um período mínimo de 30 dias atrás;

1.1.17.38. Deverá ser configurada para habilitar todos os seus servidores a reconhecer o site de origem, seus conteúdos estáticos (CSS, JS, documentos, Imagem, vídeo, áudio, dentre outros) e dinâmicos, tanto no Brasil quanto no exterior.

1.1.17.39. Deverá manter a parte estática do conteúdo dos sites disponíveis, mesmo quando ele não estiver disponível por um tempo.

1.1.17.40. Não deverá existir limite de criação de URL pertencentes à CONTRATANTE, registradas sob domínios "ce.gov.br" e "CONTRATANTE.ce.gov.br" com possibilidade de obter regras de WAF (Web Application Firewall), diferentes as regras do domínio principal.

1.1.17.41. Deverá prover disponibilidade dos sites e tempo de carga das páginas inferior ao de carga sem o uso da CDN, independentemente da quantidade de usuários e dados acessados simultaneamente.

1.1.17.42. A disponibilidade deve ser assegurada mesmo em caso de realização de testes de carga pela CONTRATANTE.

1.1.17.43. Deverá garantir o desempenho dos acessos através da determinação, em tempo real, de qual servidor de rede CDN possui melhores condições de entrega para cada usuário do conteúdo da aplicação acessada.

1.1.17.44. Deverá propagar as mudanças realizadas no dashboard em até 5 (cinco) minutos, permitindo assim a resposta a incidentes de segurança através da infraestrutura da Contratada.

1.1.17.45. Deverá realizar a expiração de conteúdo (purge) por URL, com suporte a wildcard, em toda a rede, em um prazo máximo de 5 (cinco) minutos.

1.1.17.46. Deverá possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços bem como ao serviço de origem.

1.1.17.47. Deverá acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance.

1.1.17.48. Para a aceleração e distribuição de aplicações HTTPS, a contratada deverá realizar, sem custos adicionais para a CONTRATANTE, a emissão dos certificados digitais necessários para o funcionamento de endereços em SSL.

1.1.17.49. Após a configuração de cada endereço, deverão ser realizado testes utilizando a ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest/), na qual deverá ser obtida, no mínimo, a qualificação "A".

1.1.17.50. Os Certificados Digitais A1 SSL/TLS para Servidor Web deverão ter as seguintes especificações: Os certificados emitidos deverão ser do tipo A1 SSL/TLS para Servidor Web, podendo ser individualizados para cada URL implantada ou do tipo WildCard onde o certificado permite que seja adicionada segurança SSL a ilimitados sites, desde que façam parte de subdomínios de um mesmo domínio. (Deverão ser suportados, pelo menos, os domínios do Governo do Estado do Ceará).

1.1.17.51. Todos os certificados emitidos deverão possuir o certificado raiz da autoridade certificadora dentre as que já vêm previamente instaladas e configuradas nos principais navegadores e dispositivos do mercado suportando, no mínimo: Mozilla Firefox, Google Chrome, Internet Explorer, Safari, iPhone, Android e Windows Phone.

1.1.17.52. A validade do certificado deverá ser de, no mínimo, 12 (doze) meses.

1.1.17.53. O procedimento para validação dos certificados deverá ser on-line ou telefônico.

1.1.17.54. Possuir validação da organização emissora do certificado digital, incluindo os dados da CONTRATANTE, conforme o caso, no certificado digital. Não serão aceitos certificados Let's Encrypt.

1.1.17.55. Deverá fornecer o serviço de balanceamento de carga entre links da origem, permitindo definir o peso e outras métricas.

1.1.17.56. Deverá ser capaz de identificar falhas, caso haja indisponibilidade em um dos links usados no Data Center de origem, para contínua transmissão e entrega do conteúdo.

1.1.17.57. Deverá realizar o balanceamento de tráfego por Round-Robin, ou outro algoritmo de balanceamento, assim como suportar a configuração de uma origem principal e outra backup (standby), que só será utilizada em caso de falha da primeira.

1.1.17.58. Deverá tratar os erros e exceções na comunicação a nível de rede ou de aplicação com as origens, buscando conexão nas demais origens em caso de timeout ou em caso da resposta HTTP com erro 404 (Not Found) ou 5xx.

1.1.17.59. Deverá possuir armazenamento de cache hierárquico, automaticamente ou manualmente, de todo o conteúdo estático de portais publicados, bem como replicação automática de cache em data centers globais.

1.1.17.60. Deverá limpar todo o cache armazenado na rede de entrega de conteúdo ou depurar um arquivo específico em menos de 30 (trinta) segundos usando o console ou API.

1.1.17.61. Deverá permitir a seleção de argumentos de query strings e cookies para armazenamento de objetos em cache, fazendo com que o objeto armazenado em cache seja o mesmo para solicitações com características afins.

1.1.17.62. Deverá permitir a criação de políticas de cache que permitam não fazer cache da requisição (bypass) assim como encaminhar os cookies tal como enviados pelos usuários para os servidores de origem.

1.1.17.63. Deverá ser capaz de responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS.

1.1.17.64. Deverá ser capaz de restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados.

1.1.17.65. Deverá ser capaz de modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os Data Centers de origem.

1.1.17.66. Deverá permitir a implementação de redirecionamento HTTP otimizando a comunicação com o Data Center de origem.

1.1.17.67. Deverá fornecer o serviço de Geo Localização a nível de país, que permitirá o gerenciamento de whitelist e blacklist para países não habilitados.

1.1.17.68. Deverá permitir a otimização do Tráfego IP, onde tal otimização deve ser roteada automaticamente, com base na localização da origem da solicitação através da infraestrutura tecnológica do provedor. Devendo distribuir o tráfego para reduzir a latência e melhorar o desempenho das solicitações.

1.1.17.69. Deverá realizar a entrega de qualquer formato e tipo de conteúdo nos protocolos HTTP 1.0, 1.1 e 2.

1.1.17.70. Deverá realizar a entrega do conteúdo em cache, mesmo que já expirado, caso a origem do Datacenter esteja inacessível.

1.1.17.71. Deverá prover aceleração através da compressão de dados (gzip) desde que suportado pelo navegador ou dispositivo u lizado pelo usuário.

1.1.17.72. Deverá detectar as características dos dispositivos através das informações de navegador de Internet.

1.1.17.73. Deverá permitir a otimização e a implantação de conteúdo da Web através do JavaScript assíncrono, para suportar diferentes navegadores da Web ou dispositivos móveis.

1.1.17.74. Deverá permitir a obtenção de objetos cacheados a par r de outros produtos, evitando assim conexão com o Data Center de origem.

1.1.17.75. Deverá ser capaz de verificar que a requisição está sendo feita por um site autorizado a ter acesso ao conteúdo armazenado.

1.1.17.76. Deverá prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos.

1.1.17.77. Deverá fornecer no painel de monitoramento uma ferramenta para geração de filtros, possibilitando a criação de relatórios on-line customizados por site e data, incluindo: análise de tráfego, solicitações da Web e ameaças detectadas nos vários sites publicados em domínios de clientes com uma frequência mínima de coleta de dados de 1 (um) minuto.

1.1.17.78. Deverá apresentar no painel de monitoramento, que permite acompanhar, o quantitativo de requisições realizadas para cada site WEB.

1.1.17.79. Deverá disponibilizar informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência. Deve conter ainda, informações acerca das atividades maliciosas processadas, apresentando: quais sites WEB estão sendo atacados e o que está sendo explorado no ataque.

1.1.17.80. Deverá suportar conexões de endereço IP recebidas IPv4 e IPv6 sem exigir configurações adicionais na infraestrutura tecnológica do cliente usando um gateway IPv6 (IPv6 Gateway).

1.1.17.81. Deverá apresentar no painel de monitoramento, com delay máximo de 5 (cinco) minutos, as informações e permitir a consulta de até 3 (três) dias de dados processados.

1.1.17.82. Deverá apresentar e contabilizar, através de gráficos, todas as requisições de conteúdo realizadas pelo usuário final para todo e qualquer código de status HTTP/HTTPS, gerando relatórios por período, permitindo a identificação dos picos de acesso.

1.1.17.83. Deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegados e requisições entre a CDN e o usuário final para todo e qualquer código de status HTTP/HTTPS.

1.1.17.84. Deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado, e requisições buscadas a partir da origem ou entregues a partir dos servidores de borda.

1.1.17.85. Deverá disponibilizar os Logs das informações dos servidores para download em intervalo não superior a 1 (uma) hora.

1.1.17.86. Deverá suportar o envio de informações de conexão em tempo real para a infraestrutura centralizada da origem.

1.1.17.87. Deverá possuir funcionalidade para otimização de rotas na Internet;

1.1.17.88. Deverá possuir métodos de mitigação de DoS L7 baseado em:

- **1.1.17.88.1.** Descarte de todas as requisições de um determinado IP e/ou país suspeito;
- **1.1.17.88.2.** Possuir a lista de delegação de IPs públicos, identificando país de origem da requisição;

1.1.17.89. Deverá implementar mecanismos capazes de mitigar quaisquer ataques que façam o uso não autorizado de recursos relativos ao (s) sítio (s) protegido (s), automaticamente, tanto para IPv4 e IPv6, para no mínimo:

- **1.1.17.89.1.** Ataques de inundação ou volumétricos;
- **1.1.17.89.2.** Ataques que utilizam falsificação de endereços IP de origem (IP spoofing);

1.1.17.90. Deverá ser capaz de mitigar ataque de baixa velocidade;

1.1.17.91. Deverá prover controles para evitar solicitações/requisições excessivas, por meio da utilização dos seguintes limitadores abaixo:

- **1.1.17.91.1.** IP/CIDR;
- **1.1.17.91.2.** User-agent;
- **1.1.17.91.3.** Cookie;
- **1.1.17.91.4.** Número do AS;
- **1.1.17.91.5.** Método HTTP;

1.1.17.92. Não será aceito bloqueio de ataques DoS e DDoS por ACLs em roteadores de borda da CONTRATADA;

1.1.17.93. Deverá prover mecanismos para a detecção, tratamento e prevenção ao uso de bots maliciosos;

1.1.17.94. Deverá diferenciar visitantes legítimos de ataques de bot e aplicar o tratamento adequado, visando mitigar ataques de bots identificados como maliciosos;

1.1.17.95. Deverá permitir o tratamento de bots de forma manual e automatizada por meio de controles padronizados e customizados provendo a possibilidade de criação de alertas e bloqueio, podendo retorn código de erro HTTP 403 (acesso negado) e retornar com mensagem customizada ou fornecer conteúdo alternativo e respostas customizáveis;

1.1.17.96. Deverá ser capaz de detectar congestionamentos na Internet em tempo real e realizar o roteamento de tráfego pelos caminhos menos congestionados de forma a acelerar o acesso aos sítios protegidos;

1.1.17.97. Deverá prover proteção para API, garantindo a inspeção automatizada de solicitações a APIs, proteção de APIs por rate control, listas de negação e inspeção automatizada de solicitações;

1.1.17.98. A solução de segurança deve garantir alta disponibilidade, inspeção, tratamento e eliminação de tráfego malicioso e distribuição de conteúdo, não havendo limitação do número de URLs ou URLs SSL protegidas dentro do mesmo domínio DNS ou seus subdomínios, com as seguintes funcionalidades:

- **1.1.17.98.1.** Alta disponibilidade de DNS (Domain Name System);
- **1.1.17.98.2.** Aceleração de resolução DNS;
- **1.1.17.98.3.** Interceptação e inspeção de conexões HTTPS;
- **1.1.17.98.4.** Monitoramento de usuários;

1.1.18. ITEM 18 - SERVIÇOS ESPECIALIZADOS EM SEGURANÇA (UST)

1.1.18.1. O serviço especializado será demandado através de consumo por unidade de serviço técnico (UST) mediante Ordens de Serviço (OS) prevendo o quantitativo a serem consumidos, o período de execução e a descrição dos serviços a serem executados.

1.1.18.2. O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculadas ao item da OS Qualquer alteração na quantidade de UST's deverá ser justificada e previamente aprovada pela CONTRATANTE.

1.1.18.3. Os serviços proporcionais de gerenciamento de projetos e liderança técnica deverão estar incluídos dentro do valor da hora.

1.1.18.4. O serviço especializado abrange, entre outras, as seguintes atividades:

1.1.18.4.1. Elaboração de documentação técnica e de usuário;

1.1.18.4.2. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE.

1.1.18.4.3. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas.

1.1.18.4.4. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;

1.1.18.4.5. Realização de operação assistida e monitoramento de ambientes entregues com a solução.

1.1.18.4.6. Orientar na utilização dos softwares instalados no CONTRATANTE com a utilização das melhores práticas e orientações dos fabricantes;

1.1.18.4.7. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no CONTRATANTE minimizando impactos;

1.1.18.4.8. Apoiar na configuração/parametrização do sistema em novas máquinas;

1.1.18.4.9. Orientar no levantamento de informações que possibilite a identificação de novas necessidades detectadas no ambiente do CONTRATANTE;

1.1.18.4.10. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;

1.1.18.4.11. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning disponibilidade e confiabilidade em ambientes;

1.1.18.4.12. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;

1.1.18.4.13. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE;

1.1.18.4.14. Esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE.

1.1.18.4.15. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;

1.1.18.4.16. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;

1.1.18.4.17. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;

1.1.18.4.18. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;

1.1.18.5. DA COMPLEXIDADE DO SERVIÇO

1.1.18.5.1. A adoção do valor de referência único facilita à contabilização dos serviços, todavia, demanda a definição dos parâmetros relativos a ponderação aplicável ao dimensionamento do serviço; nesse sentido, para efeito de cada projeto a ser contratado, serão adotados os seguintes pesos de complexidade:

Complexidade	Serviços	Peso Complexidade
Baixa	Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas; corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes e atividades similares.	1,0
Intermediária	Elaboração de documentação técnica e de usuário; diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos e atividades similares.	1,05
Alta	Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes; otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados; esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE; apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta e atividades similares.	1,10
Especialista	Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE; apoiar no planejamento, na execução e na avaliação das mudanças no ambiente; analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente; apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente e atividades similares.	1,15

Tabela 1 - Definições de complexidade do serviço

1.1.18.6. DAS CONDIÇÕES DE EXECUÇÃO

1.1.18.6.1. O objeto desta especificação técnica tem por escopo serviços de natureza contínua, prestados sob demanda, para serviços técnicos especializados de segurança, que venham a ser necessários a efetivação dos objetivos estratégicos da CONTRATANTE e seus clientes finais no que dependam da tecnologia da informação e comunicação.

1.1.18.6.2. A CONTRATANTE poderá a seu critério utilizar as USTs contratadas para a execução de serviços continuados (processos) ou pontuais (projetos) sem ônus ao objeto contratual, considerando especificações do catálogo de serviços.

1.1.18.7. DA SOLICITAÇÃO DE SERVIÇOS

1.1.18.7.1. Mensalmente ou em caso de necessidade serão abertas ordens de serviço, com os Serviços Técnicos devidamente identificados e associados a uma estimativa (UST) relacionadas aos serviços a serem executados.

1.1.18.7.2. A partir da abertura da OS, todas as atividades necessárias para a execução dos serviços deverão estar relacionadas às demandas devidamente registradas em ferramenta de Gestão de Demandas. Quando não houver disponibilidade desta ferramenta, poderá ser realizada por qualquer outra compatível.

1.1.18.7.3. Para o encerramento de uma demanda é necessário o registro das atividades que evidenciam o seu atendimento.

1.1.18.7.4. O cálculo do número de USTs relativas aos serviços solicitados, será realizado por ocasião da emissão da ordem de serviços (OS) que poderá contemplar a execução de um ou mais serviço. Esse agrupamento só deverá ser aplicado para serviços com durações semelhantes, para não ocasionar retardo no encerramento da OS. O referido cálculo deverá ser feito para cada serviço solicitado na OS conforme a seguinte fórmula:

UST= (Esforço x complexidade)

onde:

UST: corresponde ao quantitativo de unidades de serviços técnicos estimados para a realização do serviço.

Esforço: Somatório da estimativa de todos esforços decorrentes da alocação temporal de um ou mais recursos necessários ao serviço, considerados os pesos aplicados a cada recurso. Ou seja, **Esforço = Fator* Número de horas alocadas.**

Complexidade: peso quanto ao tipo predominante de atividades inerentes a sua realização do serviço.

1.1.18.7.5. Para aplicação da fórmula da UST ajustada por serviço, deve-se considerar que:

1.1.18.7.5.1. O dimensionamento do esforço para o serviço demandará estudo para definição de estimativas da alocação recursos necessários ao serviço, considerando quantitativos e a alocação temporal dos recursos para atendimento demanda.

1.1.18.7.5.2. A CONTRATADA poderá adotar o fator médio de 1,368 do ANEXO C para dimensiona o esforço;

1.1.18.7.5.3. Caso opte por não usar o fator médio a CONTRATADA deverá dimensionar o esforço adotando os pesos definidos no ANEXO C - LISTA DE PERFIS TÉCNICOS dos recursos.

ANEXO C - LISTA DE PERFIS TÉCNICOS

1. A tabela a seguir estabelece relação entre os perfis técnicos dos recursos a serem alocados na execução dos serviços, sejam profissionais ou materiais, com o peso adotado do para efeito de cálculo do esforço considerado no dimensionamento de USTs do serviço.

Item	Perfil Técnico	Requisitos Técnicos Mínimos Obrigatórios de Enquadramento	Peso
1	Auxiliar Técnico I	**Do Auxiliar Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 01 (um) ano em atividades e funçõescorrelatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto daatividade, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço.	0,25
2	Auxiliar Técnico II	**Do Auxiliar Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível médio emqualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto daatividade, com experiência comprovada e no mínimo 02 (dois)anos em atividades e funções correlatas ao serviço.	0,50

3	Técnico I	**Do Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 03 (três) anos em atividades e funções correlatas aoserviço. **Do Técnico de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível médio emqualquer área compatível área compatível com o processo denegócio objeto da atividade, com experiência mínima de, 03 (três) anos em atividades e funções correlatas ao serviço.	1
4	Técnico II	**Do Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível superiorem andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço com experiência comprovada de no mínimo 03 (três)anos em atividades e funções correlatas ao serviço. Ou Alternativamente, profissionais com formação de nível médioem qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 05 (cinco) anos em atividades e funções correlatasao serviço. **Do Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço. Ou Alternativamente, profissionais com formação de nível médioem qualquer em área compatível com o processo de negócio objeto da atividade, com	1,5

		experiência comprovada mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço.	
5	Analista I	**Do Analista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superiorem área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 05 (cinco) anos em atividades e funções correlatas ao serviço, **Do Analista de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível superiorcompatível com o processo de negócio objeto da atividade, com experiência mínima de 05 (cinco) anos em atividades efunções correlatas ao processo objeto da atividade.	2,0

6	Analista II	**Do Analista de TIC de Nível II** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com as técnicas e tecnologiasaplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível comas técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao serviço. **Do Analista de Processo de Negócio Nível II** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 08 (oito) anos em atividades e funções correlatas aoprocesso objeto da atividade.	2,50

7	Especialista I	**Do Especialista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 07 (sete) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível comas técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas aoserviço. **Do Especialista de Processo de Negócio Nível I** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Lato Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 07 (sete) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível como processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	3,00

8	Especialista II	**Do Especialista de TIC de nível II** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Stricto Sensu) compatível com astécnicas e tecnologias aplicadas às atividades inerentes ao serviço e experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao serviço, Ou, Alternativamente, formação de nível superior e pós-graduação(no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas aoserviço. **Do Especialista de Processo de Negócio nível II** Enquadram-se os profissionais com formação de nível superiore pós-graduação (no mínimo Stricto Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade; Ou, Alternativamente, formação de nível superior e pós-graduação(no mínimo Lato Sensu) compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividadese funções correlatas ao processo objeto da atividade.	3,50

3. Com vistas a favorecer o processo de precificação do serviço no que se refere a alocação de recursos necessários ao serviço, considerada a necessidade de execução contínua de dadas atividades, a aceitabilidade definida dos perfis por serviços relacionados no catálogo de

serviços, e cenários atuais relativos aos serviços demandados, estima-se que para correta execução dos serviços, os recursos necessários serão alocados com base na seguinte distribuição de tempo:

Perfil Técnico	Alocação estimada
Auxiliar I	17%
Auxiliar II	17%
Técnico I	16%
Técnico II	16%
Analista I	16%
Analista II	8%
Especialista I	5%
Especialista II	5%

4. Considerando os serviços listados no catálogo, seus pesos e distribuições adote-se apenas como referência para precificação, o fator médio de 1,368 para conversão entre horas de alocação e UST conforme a seguinte fórmula: Número de horas alocadas = (Número de UST_mês/(1,368*COMPLEXIDADE)). Esse fator foi definido com consideração a média de todos os pesos aplicáveis aos serviços no catálogo, permitindo uma aproximação do quantitativo em horas, da alocação necessária de recursos para a execução dos serviços.

4.1 A CONTRATADA deverá propor um fator diferente do fator médio para aqueles casos em que a alocação real não está de acordo com a alocação estimada, o qual será avaliado pela CONTRATANTE.

ANEXO D - CATÁLOGO DE SERVIÇOS

O catálogo de serviços apresentado na tabela abaixo lista as complexidades esperadas para cada serviço a ser executado.

Este catálogo pode ser alterado pontualmente na medição de serviços no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para uma determinada atividade uma complexidade diferente da listada.

Este catálogo pode ser alterado continuamente no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para a maioria das atividades relacionadas a ele uma complexidade diferente da listada.

SERVIÇO	COMPLEXIDADE
Avaliação e descoberta de portfólio de aplicações e suas interdependências para construção de plano para migração.	Intermediário
Avaliação de infraestrutura existente para dimensionamento deinfraestrutura necessária em ambiente de nuvem.	Intermediário
Migração de cargas de trabalho entre sistemas operacionais(Linux/ Windows)	Intermediário
Migração de cargas de trabalho entre bancos de dados heterogêneos .	Alta
Migração de bases de dados on-premises para nuvem, com ou sem atualização de versão, para: outros motores suportados; bases de dados para propósitos específicos (NoSQL).	Alta
Migração de containers on-premises para soluções de orquestração e repositório de containers gerenciados.	Alta
Migração de cargas de trabalho, elegíveis, de máquinas virtuaispara containers.	Alta
Migração de cargas de trabalho, elegíveis, máquinas virtuais oucontainers para modelo sem servidor.	Alta
Migração de cargas de trabalho em máquinas virtuais para serviços gerenciados e não gerenciados elegíveis.	Alta
Implementação de mecanismo de alta disponibilidade, escalabilidade horizontal automatizada, monitoramento, verificações de saúde e balanceamento de carga.	Alta
Construção de data warehouse e/ou datamarts a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista

Construção de soluções de analytics a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Construção de soluções de Big Data a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Desenvolvimento e implementação de projetos que envolvem tecnologias de Inteligência Artificial, linguagens e aprendizado de máquina, redes neurais, preditivas e demais tecnologiasenvolvidas.	Especialista
Desenvolvimento e implementação de projetos de atendimento virtual, robôs e demais ferramentas de conversação inteligente automatizada.	Especialista
Desenvolvimento e implementação de projetos que envolvemsoluções de IoT (Internet das Coisas).	Especialista
Implementação de rede de entrega de conteúdo para conteúdo(site) estáticos.	Intermediário
Criação/configuração de topologia de redes interconectadas com isolamento, firewall, ACL's (Access Control Lists) e auditoria.	Intermediário
Implementação e configuração de conectividade do ambienteon-premises com ambiente em nuvem.	Intermediário
Configuração de serviço de DNS, público ou privado, e integração com serviço de DNS on-premises.	Intermediário
Implementação de modelo de categorização de custos combase em rótulos, orçamentos e alarmes de consumo mensal.	Baixa
Implementação de controles para filtro de requisições Web classificadas como nocivas.	Intermediário
Configuração de cofre de senhas para armazenamento de credenciais, chaves e outros dados sensíveis.	Intermediário
Automação do provisionamento e gerência de configuração de serviços e recursos de nuvem com modelo de infraestrutura como código e autosserviço.	Alta
Implementação de solução para gerenciamento e automaçãode backup de dados nos serviços de nuvem ou ambiente on-premises.	Intermediário
Implementação de solução para backup de dados de longa retenção com políticas de ciclo de vida.	Intermediário

Implementação de processos de transferência de grandes volumes de dados para nuvem, incluindo processo de backup e restauração em novo ambiente.	Intermediário
Desenho e implantação de arquitetura para continuidade de negócios e recuperação de desastres em ambiente de nuvemde acordo com requisitos de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).	Especialista
Apresentação de workshops/transferência de conhecimentopara detalhamento de entregáveis.	Baixa
Configuração de estrutura de contas em conformidade commelhores práticas de segurança.	Intermediário
Avaliação de ambiente em nuvem sobre perspectiva de segurança, desempenho, confiabilidade, custos e eficiência operacional e aplicação de correções apropriadas.	Alta
Migração fim-a-fim de máquinas virtuais incluindo os processos de conversão, importação, configuração e testes do ambiente migrado.	Alta
Implementação de ambiente para virtualização de desktops,incluindo configuração de redes, autenticação, políticas de gerenciamento e imagens personalizadas com configurações e aplicativos.	Alta
Gerenciamento dos provedores de serviço, orquestração, bilhetagem, implementação de mecanismos de controle, otimização de custos, sustentação e operação de ambiente de Nuvem com execução de tarefas do dia a dia: monitoramento, aplicações de patches, backup, atendimento de requisições de tarefas e mudanças.	Baixa
Serviço de monitoramento dos recursos e componentes da solução.	Baixo

ANEXO E - MODELO DA PROPOSTA DE PREÇOS

Tabela 1 - Cessão de direito de Uso de Software para Nuvem

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD (A)	VALOR UNIT MENSAL (B)	VALOR ANUAL (C = A x B x 12)
1	SOLUÇÃO DE NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA OU NUVEM PRIVADA	LICENÇA	40		
2	SOLUÇÃO DE AUTOMAÇÃO DE GOVERNANÇA, POSTURA E CONFORMIDADE PARA NUVENS PÚBLICAS	LICENÇA	8		
3	SOLUÇÃO DE PROTEÇÃO PARA APLICAÇÕES WEB EM NUVEM (WAF), DEFESA DE API E AUTOMAÇÕES (BOTS)	PACOTES DE 100 MILHÕES DE REQUISIÇOES	30		
4	SOLUÇÃO PARA ANÁLISE DE SEGURANÇA EM DESENVOLVIMENTO DE CÓDIGO FONTE	PACOTES DE 25 DEVELOPERS	20		
5	SOLUÇÃO DE ANÁLISE E GESTÃO INTELIGENTE DE VULNERABILIDADE PARA RECURSOS DE NUVEM	PACOTES DE 300 ATIVOS	10		
6	SOLUÇÃO PARA INSPEÇÃO DE TRÁFEGO E ACESSO SEGURO À INTERNET	LICENÇA	5.000		
7	SOLUÇÃO DE MONITORAMENTO DE EXPERIÊNCIA CONTÍNUA DOS USUÁRIOS	LICENÇA	5.000		
8	SOLUÇÃO PARA ACESSO SEGURO A APLICAÇÕES PRIVADAS	LICENÇA	5.000		
9	SOLUÇÃO DE SEGURANÇA DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM	LICENÇA	1.000		
10	SOLUÇÃO DE PROTEÇÃO E SEGURANÇA DE DADOS	Terabyte (TB)	300		
11	SOLUÇÃO DE PROTEÇÃO PARA AMBIENTES COLABORATIVOS	PACOTES DE 500 USUÁRIOS	10		
12	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – MONITORAMENTO E MITIGAÇÃO DE RISCOS ÀS IDENTIDADES DA TI	LICENÇA	200		
13	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA SERVIDORES WINDOWS E LINUX/UNIX	LICENÇA	500		
14	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – PROTEÇÃO PARA ESTAÇÕES	LICENÇA	2.000		
15	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – AUTENTICAÇÃO MULTI-FATOR COM INTELIGÊNCIA DE AMEAÇAS	LICENÇA	2.000		
16	SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS NA NUVEM – GERENCIAMENTO DE CREDENCIAIS DAS IDENTIDADES DO USUÁRIO FINAL	LICENÇA	2.000		

17	PLATAFORMA DE REDE DE DISTRIBUIÇÃO DE CONTEÚDO - CDN	PACOTES DE 5 TERABYTES (TB)	8		
Soma (d)					

(t1)Valor Total em R$ (igual a "d")

_____

Tabela 2 – Serviços Técnicos

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD Anual (A)	VALOR UNIT (B)	VALOR ANUAL (C = A x B)
18	SERVIÇOS ESPECIALIZADOS EM SEGURANÇA	UST	30.000		
Soma (d)					

(t2)Valor Total em R$ (igual a "d")

_____

Valor Total da Proposta (t1 +t2)

_____