CLAUDIA SANT ANNA PINHEIRO:97500
14/10/2024 16:11

MARCIO NISI GONCALVES:47597
14/10/2024 19:13

AQUILES JOSE MALVEZZI:78700
15/10/2024 12:09

VALDIR FLORINDO:103870
15/10/2024 17:42

JOSE ANDRE MENDES COIMBRA:47153989153
16/10/2024 10:41

PROAD Nº 22.093/2024 - CONTRATO N° 097/2024

CONTRATO QUE FAZEM ENTRE SI O TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO E O CONSÓRCIO PETASERVICE SEC., PARA A PRESTAÇÃO DE SERVIÇOS DE MONITORAMENTO, DETECÇÃO, NOTIFICAÇÃO, INVESTIGAÇÃO E RESPOSTA A ATAQUES CIBERNÉTICOS.

O **TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO,** Órgão do Poder Judiciário Federal, Justiça do Trabalho, com sede na Rua da Consolação, 1.272, São Paulo/SP, inscrito no CNPJ sob o nº 03.241.738/0001-39, neste ato representado por seu Desembargador Presidente, doravante denominado simplesmente **CONTRATANTE** e, de outro lado, o **CONSÓRCIO PETASERVICE SEC.**, inscrito no CNPJ sob o nº 57.413.479/0001-05, com endereço em SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília-DF - CEP 70.200-002, e-mail: juridico@petacorp.com.br, doravante designada **CONTRATADA**, neste ato representada pelo(a) Sr. José André Mendes Coimbra, na presença de duas testemunhas, celebram o presente contrato, decorrente do **Pregão Eletrônico nº 030/2024**, em conformidade com o **PROAD nº 22.093/2024**, e em observância às disposições da Lei n.º 14.133, de 1º de abril de 2021, bem como demais legislações aplicáveis, firmando o compromisso de cumpri-lo de acordo com as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA: DO OBJETO

O objeto do presente contrato é a contratação de serviços de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, nas condições estabelecidas na Especificação do Objeto.

Parágrafo Único: Vinculam esta contratação, independentemente de transcrição:

I – A Especificação do Objeto;

II - O Edital da Licitação;

III - A Proposta da **CONTRATADA**;

IV - Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA: DA VIGÊNCIA, DA EXECUÇÃO DOS SERVIÇOS E DA PRORROGAÇÃO

O prazo de vigência deste contrato terá início na data de sua assinatura, com a prestação dos serviços pelo período de 24 (vinte e quatro) meses, contados a partir do recebimento definitivo do serviço de implantação da solução, descrita no item 4 do Anexo I.

Parágrafo Primeiro: O prazo de vigência disposto no *caput* poderá ser prorrogado por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133/2021.

Parágrafo Segundo: A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para o **CONTRATANTE**, permitida a negociação com a **CONTRATADA**.

Parágrafo Terceiro: A prorrogação do prazo de vigência será precedida de verificação da regularidade fiscal da **CONTRATADA**, consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e ao Cadastro Nacional de Empresas Punidas (CNEP), emissão das certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas.

CLÁUSULA TERCEIRA: DOS MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

O regime de execução desta contratação é a empreitada por preço global.

Parágrafo Único: As demais condições de execução estão dispostas no Anexo I – Especificação do Objeto.

CLÁUSULA QUARTA: DA SUBCONTRATAÇÃO

Não será admitida a subcontratação total ou parcial do objeto.

CLÁUSULA QUINTA: DO VALOR DO CONTRATO

Os valores desta contratação são:

GRUPO 1 (G1)									
Item	**Descrição**	**Faixa**	**Faixa de subscrição por ativo**	**Unidade de medida**	**Qtde.**	**Valor unitário único**	**Valor unitário anual**	**Valor unitário mensal**	**Valor total (24 meses)**
5	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	9864	-	R$ 139,23	-	R$ 2.746.729,44
6		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	2	-	R$ 126.056,50	-	R$ 504.226,00
7	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes	Serviço pontual, por turma de treinamento (8 alunos por turma no	1	R$ 6.000,00	-	-	R$ 6.000,00

GRUPO 1 (G1)									
Item	**Descrição**	**Faixa**	**Faixa de subscrição por ativo**	**Unidade de medida**	**Qtde.**	**Valor unitário único**	**Valor unitário anual**	**Valor unitário mensal**	**Valor total (24 meses)**
				máximo)					
8	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	1	R$ 30.500,00	-	-	R$ 30.500,00
13	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	-	-	R$ 35.833,33	R$ 860.000,00

Parágrafo Único: Nos valores acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, bem como taxas de licenciamento, administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA SEXTA: DO PAGAMENTO

O pagamento será efetuado em até 5 (cinco) dias úteis contados da data da liquidação da despesa.

Parágrafo Primeiro: O pagamento referente aos serviços de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 9 a 13 da tabela do item 1 do Anexo I) será proporcional ao atendimento das metas estabelecidas no Acordo de Nível de Serviço, conforme disposto nos itens 5.22 e 5.24 a 5.28 do Anexo I.

Parágrafo Segundo: Ocorrerá a glosa no pagamento devido, sem prejuízo das sanções cabíveis, quando a **CONTRATADA** não produzir os resultados ou não executar com a qualidade mínima exigida as atividades contratadas, conforme disposto no Instrumento de Medição de Resultado.

Parágrafo Terceiro: A **CONTRATADA** poderá discriminar na nota fiscal/fatura o valor total de desconto por eventual descumprimento do Instrumento de Medição de Resultado ocorrido no mês de referência e faltas, efetuando o devido abatimento no valor da nota fiscal/fatura.

Parágrafo Quarto: Havendo erro na apresentação da nota fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras. Nesta hipótese, o prazo para liquidação iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o **CONTRATANTE**.

Parágrafo Quinto: A liquidação da despesa só ocorrerá após a comprovação da manutenção das condições de habilitação exigidas.

Parágrafo Sexto: Em caso de irregularidade fiscal haverá suspensão do prazo de liquidação e a **CONTRATADA** será notificada para que sejam sanadas as pendências no prazo de 5 (cinco) dias úteis, prorrogável por igual período.

Parágrafo Sétimo: O pagamento será creditado em favor da **CONTRATADA** por meio de ordem bancária, na instituição bancária indicada no cadastro realizado no SIGEO-JT.

Parágrafo Oitavo: O **CONTRATANTE** poderá efetuar o pagamento por meio de títulos de cobrança bancária com código de barras, desde que o valor seja líquido, já descontada a retenção na fonte prevista neste instrumento.

Parágrafo Nono: O pagamento por meio de títulos de cobrança bancária com código de barras não isenta a **CONTRATADA** da apresentação do respectivo documento fiscal.

Parágrafo Dez: Sobre o valor faturado, serão retidos na fonte os correspondentes tributos e contribuições, conforme legislação aplicável.

Parágrafo Onze: A empresa optante pelo regime do Simples Nacional deverá encaminhar declaração nos moldes exigidos pela Receita Federal do Brasil antes da emissão da primeira Nota Fiscal Eletrônica, para fins de comprovação de sua situação jurídica, sendo de sua inteira responsabilidade informar eventual desenquadramento do regime, sob pena da incidência das penalidades previstas neste instrumento.

Parágrafo Doze: Considera-se como data do efetivo pagamento o dia em que for emitida a competente ordem bancária em favor da **CONTRATADA**.

Parágrafo Treze: O **CONTRATANTE** poderá deduzir, cautelar ou definitivamente, do montante a pagar à **CONTRATADA**, os valores correspondentes a multas, ressarcimentos ou indenizações devidas pela **CONTRATADA**, nos termos deste contrato.

Parágrafo Catorze: No caso de atraso de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, serão devidos pelo **CONTRATANTE** encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime

de juros simples, mediante solicitação da **CONTRATADA** em até 10 (dez) dias da emissão da Ordem Bancária, segundo a aplicação das seguintes fórmulas:

I = (TX/100)/365

EM = I x N x VP, onde:

I = Índice de apuracão dos encargos;

TX = Percentual anual de encargos moratórios;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso

CLÁUSULA SÉTIMA: DO REAJUSTE E DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 11/04/2024.

Parágrafo Primeiro: Após o interregno de um ano, e após pedido da **CONTRATADA,** os preços iniciais serão reajustados, mediante a aplicação, pelo **CONTRATANTE**, do IPCA-E, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

Parágrafo Segundo: Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

Parágrafo Terceiro: No caso de atraso ou não divulgação do índice de reajustamento, o **CONTRATANTE** pagará à **CONTRATADA** a importância calculada pela última variação conhecida, apurando-se a diferença correspondente tão logo seja divulgado o índice definitivo.

Parágrafo Quarto: Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

Parágrafo Quinto: Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

Parágrafo Sexto: Na ausência de previsão legal quanto ao índice substituto, o **CONTRATANTE** elegerá novo índice oficial, para reajustamento do preço do valor remanescente, mediante apostila.

Parágrafo Sétimo: O reajuste será realizado por apostilamento.

Parágrafo Oitavo: Os reajustes serão precedidos de solicitação da **CONTRATADA** em até, no máximo, o mês subsequente ao da aquisição do direito, ficando garantida a eficácia retroativa do pedido. Ultrapassado esse prazo, os efeitos financeiros somente terão vigência a partir da data da solicitação.

Parágrafo Nono: O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 107 da Lei nº 14.133/2021. A extinção do contrato não configurará óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

Parágrafo Dez: O **CONTRATANTE** dará resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro preferencialmente no prazo de 30 (trinta) dias úteis, após o recebimento de toda a documentação comprobatória, apta à análise do pedido para eventual deferimento/indeferimento, tais como, notas fiscais e demais documentos pertinentes que comprovem o desequilíbrio, acompanhada de demonstração analítica da variação cambial e/ou dos custos contratuais.

CLÁUSULA OITAVA: DAS OBRIGAÇÕES

São obrigações das partes:

I) Da CONTRATADA:

a) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas de qualificação;

b) Responsabilizar-se pelos encargos trabalhistas, sociais, previdenciários, fiscais e comerciais resultantes da execução dos serviços prestados;

c) Obedecer às normas técnicas de saúde, de segurança do trabalho e de proteção ao meio ambiente;

d) Assumir integral responsabilidade por quaisquer compromissos assumidos com terceiros, ainda que vinculados à execução do contrato, bem como pelos danos causados à União ou a terceiros, por seus empregados, na prestação dos serviços contratados, inclusive por acidentes, mortes, perdas ou destruições, furtos comprovados, isentando a União de todas e quaisquer reclamações que possam advir, devendo proceder aos reparos necessários ou ao pagamento de indenização correspondente;

e) Selecionar e preparar rigorosamente os empregados, instruindo-os a tratar

com urbanidade e respeito todas as pessoas presentes nas dependências do **CONTRATANTE** e de suas unidades, onde prestar serviço;

f) Manter a disciplina no local dos serviços, adotando medidas que previnam ou reprimam, de forma eficaz, condutas prejudiciais à adequada execução contratual, sob pena de aplicação das penalidades cabíveis;

g) Fornecer pessoal capacitado para a atividade, devidamente uniformizado, com seu logotipo, crachá de identificação, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência, seguindo as normas de segurança do **CONTRATANTE**;

h) Manter preposto aceito pelo **CONTRATANTE** no local da obra ou do serviço para representá-lo na execução deste contrato;

i) Cercar os seus empregados de todas as garantias e medidas de proteção ditadas pela legislação vigente, inclusive no que diz respeito à higiene e segurança do trabalho, mediante o emprego de todos os meios acautelatórios aconselhados para cada espécie de serviço a executar, responsabilizando-se pelo fornecimento e fiscalização de todos os equipamentos e materiais de proteção individual (EPI) e Coletivo (EPC), ficando sob sua inteira responsabilidade qualquer acidente ou dano que venha a ocorrer durante a execução do serviço;

j) Eximir-se de contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do **CONTRATANTE** ou de agente público que na fiscalização ou na gestão deste contrato;

k) Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

l) Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior, comunicando a estes, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

m) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

n) Prestar todo esclarecimento ou informação solicitada pelo **CONTRATANTE** garantindo-lhe o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;

o) Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

p) Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

q) Submeter previamente, por escrito, ao **CONTRATANTE**, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações inicialmente contratadas;

r) Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

s) Comprovar, sempre que solicitado, sob pena de rescisão contratual, que não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH nº 04/2016; e que não foi condenada, a **CONTRATADA** ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo.

t) Comprovar semestralmente o cumprimento, quando couber e conforme proporção, do preenchimento de seus cargos com a cota de beneficiários ou pessoas portadoras de deficiência, e incentivo à inclusão de pessoas com Síndrome de Down, conforme previsto na legislação;

u) Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

v) Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

w) Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do **CONTRATANTE**;

x) Conhecer e cumprir o Plano de Integridade/Programa de Integridade e

Compliance e o Código de Ética[1] do **CONTRATANTE**;

II) Do CONTRATANTE:

a) Prestar os esclarecimentos que eventualmente venham a ser solicitados;

b) Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;

c) Receber o objeto no prazo e condições estabelecidas no Anexo I - Especificação do Objeto;

d) Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

e) Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA** por meio de gestor/fiscais;

f) Comunicar à **CONTRATADA** para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

g) Efetuar o pagamento à **CONTRATADA** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e na Especificação do Objeto;

h) Aplicar à **CONTRATADA** as sanções previstas na lei e neste Contrato;

i) Cientificar, quando julgar necessário, o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pela **CONTRATADA**;

j) Emitir explicitamente decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

j.1) A Administração terá o prazo de 30 (trinta) dias úteis, a contar da data do protocolo do requerimento, para decidir, admitida a prorrogação motivada por igual período.

k) Recusar, desde que justificada, a indicação ou a manutenção do preposto da **CONTRATADA**, devendo esta designar outro para o exercício da atividade;

1 Disponíveis em https://ww2.trt2.jus.br/fileadmin/agep/planejamento_estrategico/Plano_de_Integridade/Plano_de_Integridade_do_TRT2_-_com_anexo_-_Versao_2.pdf e https://basis.trt2.jus.br/handle/123456789/15693

l) Comunicar à **CONTRATADA** na hipótese de posterior alteração do projeto, no caso do art. 93, §2º, da Lei nº 14.133, de 2021;

m) Exercer a mais ampla e completa fiscalização sobre os serviços, não obstante a **CONTRATADA** seja a única e exclusiva responsável pela execução do objeto, sem que de qualquer forma haja restrição à plenitude dessa responsabilidade;

n) Suspender qualquer serviço no qual se evidencie risco iminente, ameaçando a segurança de pessoas, equipamentos, patrimônio do **CONTRATANTE** ou de terceiros;

o) Assegurar o livre acesso das pessoas credenciadas pela **CONTRATADA** aos locais onde serão executados os serviços, prestando-lhes os esclarecimentos que eventualmente venham a ser solicitados.

CLÁUSULA NONA: DAS OBRIGAÇÕES PERTINENTES À LGPD

As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

Parágrafo Primeiro: Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

Parágrafo Segundo: É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

Parágrafo Terceiro: O **CONTRATANTE** deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pela **CONTRATADA**.

Parágrafo Quarto: Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da **CONTRATADA** eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

Parágrafo Quinto: É dever da **CONTRATADA** orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

Parágrafo Sexto: A **CONTRATADA** deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

Parágrafo Sétimo: O **CONTRATANTE** poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a **CONTRATADA** atender prontamente eventuais pedidos de comprovação formulados.

Parágrafo Oitavo: A **CONTRATADA** deverá prestar, no prazo fixado pelo **CONTRATANTE**, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

Parágrafo Nono: Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

Parágrafo Dez: Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pelo **CONTRATANTE** nas hipóteses previstas na LGPD.

Parágrafo Onze: O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA DEZ: DA GARANTIA DE EXECUÇÃO

Não haverá exigência de garantia contratual da execução.

CLÁUSULA ONZE: DAS SANÇÕES ADMINISTRATIVAS

Comete infração administrativa a **CONTRATADA** que:

I - der causa à inexecução parcial do contrato;

II - der causa à inexecução parcial do contrato que cause grave dano ao **CONTRATANTE**, ao funcionamento dos serviços públicos ou ao interesse coletivo;

III - der causa à inexecução total do contrato;

IV - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

V - prestar declaração falsa durante a execução do contrato;

VI - praticar ato fraudulento na execução do contrato;

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

VIII - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

IX - praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

Parágrafo Primeiro: Nas hipóteses de cometimento de qualquer infração administrativa, assegurada a ampla defesa e o contraditório, poderão ser aplicadas à **CONTRATADA**, sem prejuízo da responsabilidade civil e criminal, as seguintes sanções:

a) Advertência por escrito em caso de inexecução parcial de obrigação, exclusivamente na hipótese de inexistência de conduta de má-fé, quando não se justificar a imposição de penalidade mais grave;

b) Multa:

b.1) moratória de 0,5% (cinco décimos por cento) do valor do contrato em casos de atraso injustificado na execução do contrato, por dia, exceto para o caso descrito na alínea 'b.2', e até o limite de 15% (quinze por cento);

b.1.1) O atraso superior a 30 (trinta) dias autoriza o **CONTRATANTE** a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

b.2) moratória de 0,5% (cinco décimos por cento) do valor do contrato caso a **CONTRATADA** apresente os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas (item 5.29 e subitens do Anexo I) em prazo superior a 20 (vinte) dias úteis até o limite de 30 (trinta) dias úteis. Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto;

b.3) compensatória de 1% (um por cento) do valor do contrato caso a disponibilidade de toda a infraestrutura necessária à prestação dos serviços tenha valor apurado de 99% (noventa e nove por cento) por mês até o limite de 95% (noventa e cinco por cento) de disponibilidade. Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto.

b.3.1) A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês.

b.4) compensatória de 0,5% (cinco décimos por cento) do valor do contrato, para cada indicador de nível de serviço (item 5.24.9 do Anexo I) que apresente discrepância superior a 50% (cinquenta por cento) até o limite de 100% (cem por cento). Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto.

b.5) compensatória de 0,5% (cinco décimos por cento) do valor do contrato, caso a **CONTRATADA** apresente discrepância superior a 20% (vinte por cento) em relação à meta prevista para mais de 3 (três) indicadores de nível de serviço (item 5.24.9 do Anexo I), até o limite de 5 (cinco indicadores). Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto.

b.6) compensatória de 1% (um por cento) do valor do contrato, caso haja execução de procedimentos, intencionais ou não, que burlem ou prejudiquem o atingimento de metas de nível de serviço. Em caso de reincidência, ensejará a inexecução parcial ou total do contrato;

b.7) compensatória de 1% (um por cento) do valor do contrato, para cada indicador/meta de níveis de serviço que tenha sido objeto de tentativa de manipulação ou descaracterização pela **CONTRATADA**. Em caso de reincidência, ensejará a inexecução parcial ou total do contrato;

b.8) compensatória de 0,5% (cinco décimos por cento) do valor do contrato, para cada ocorrência de descumprimento de obrigações contratuais que não sejam relacionadas ao atingimento das metas estabelecidas para os indicadores de nível de serviço (item 5.24.9 do Anexo I);

b.9) compensatória de 10% (dez por cento) em caso de inexecução parcial e de 30% (trinta por cento) em caso de inexecução total do valor do contrato.

b.10) compensatória de 5% (cinco por cento) do valor do contrato na hipótese de não-cumprimento de qualquer outra obrigação contratual acessória que não envolva prazo, exceto para o caso descrito na alínea 'b.8';

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta da União pelo prazo máximo de 3 (três) anos, de acordo com as penas-base dispostas no Ato GP nº 24/2022 do Tribunal Regional do Trabalho da 2ª Região.

d) Declaração de inidoneidade para licitar ou contratar, no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, de acordo com as penas-base dispostas no Ato GP nº 24/2022 do Tribunal Regional do Trabalho da 2ª Região.

Parágrafo Segundo: A penalidade de multa poderá ser aplicada por qualquer hipótese de infração administrativa, isolada ou cumulativamente com as demais espécies de sanções.

Parágrafo Terceiro: As multas previstas neste instrumento, se aplicadas,

poderão ser descontadas dos pagamentos a que porventura a **CONTRATADA** tenha direito.

Parágrafo Quarto: Caso inexistentes pagamentos ou se os valores das faturas ou garantia forem insuficientes, a **CONTRATADA** deverá recolher as multas no prazo máximo de 30 (trinta) dias, contados a partir do recebimento de notificação, por meio de GRU – Guia de Recolhimento da União, apresentando o comprovante ao **CONTRATANTE**, sob pena de inscrição na Dívida Ativa da União.

Parágrafo Quinto: A **CONTRATADA** que der causa à inexecução parcial do contrato que cause grave dano ao **CONTRATANTE**, ao funcionamento dos serviços públicos ou ao interesse coletivo, der causa à inexecução total do contrato, não mantiver a proposta ou ensejar o retardamento da execução ou da entrega do objeto, ficará impedida de licitar e contratar no âmbito da União, de acordo com as penas-base dispostas no Ato GP nº 24/2022, quando não se justificar a imposição de penalidade mais grave, sem prejuízo das multas previstas neste contrato e das demais cominações legais.

Parágrafo Sexto: A **CONTRATADA** que prestar declaração falsa durante a execução do contrato, praticar ato fraudulento na execução do contrato, comportar-se de modo inidôneo, cometer fraude de qualquer natureza ou praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013, será declarada inidônea e ficará impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, de acordo com as penas-base dispostas no Ato GP nº 24/2022, sem prejuízo das multas previstas neste contrato e das demais cominações legais.

Parágrafo Sétimo: Todas as penalidades serão registradas no SICAF, no CEIS e no CNEP.

Parágrafo Oitavo: A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

Parágrafo Nono: Todas as comunicações dos atos administrativos serão realizadas de forma eletrônica, nos endereços de e-mail fornecidos pela **CONTRATADA** no contrato ou cadastrado no SICAF, sendo de sua responsabilidade o acompanhamento e atualização dos respectivos endereços.

Parágrafo Dez: A comunicação, enviada aos endereços de correio eletrônico da **CONTRATADA**, será considerada como efetivamente realizada após 10 (dez) dias úteis, contados a partir do primeiro dia útil subsequente à data do envio, não podendo alegar desconhecimento do recebimento das comunicações por este meio como justificativa para se eximir das responsabilidades assumidas ou eventuais sanções aplicadas.

Parágrafo Onze: A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATADA,** observando-se o procedimento previsto no Ato GP nº 24/2022 do Tribunal Regional do Trabalho da 2ª Região.

Parágrafo Doze: Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159, da Lei 14.133, de 2021).

Parágrafo Treze: A personalidade jurídica da **CONTRATADA** poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a **CONTRATADA**, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia. (art. 160, da Lei nº 14.133, de 2021).

Parágrafo Catorze: As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21 e Ato GP nº 24/2022 do Tribunal Regional do Trabalho da 2ª Região.

CLÁUSULA DOZE: DA ALTERAÇÃO SUBJETIVA

É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, mediante Termo Aditivo, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do **CONTRATANTE** à continuidade do contrato.

CLÁUSULA TREZE: DAS VEDAÇÕES

É vedado à **CONTRATADA**:

a) Caucionar ou utilizar este contrato para qualquer operação financeira; e

b) Interromper a execução dos serviços/atividades sob alegação de inadimplemento por parte do **CONTRATANTE**, salvo nos casos previstos em lei.

CLÁUSULA CATORZE: DO RECEBIMENTO DO OBJETO

Em conformidade com o art. 140 da Lei nº 14.133/2021, o objeto desta contratação será recebido:

I – No caso dos serviços referentes aos itens 1 a 6 da tabela constante do Anexo I

a) **provisoriamente**, pelo responsável pelo acompanhamento e fiscalização do contrato, mediante termo detalhado, após verificação do cumprimento das exigências de caráter técnico, na data da instalação e configuração do console de gerência, dos coletores de logs, dos coletores de tráfego de rede e de agentes em estações de trabalho e em servidores;

b) **definitivamente**, no prazo de 10 (dez) dias úteis, contados do recebimento provisório, pelo servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências descritas no item 2.98 do Anexo I, além da comprovação da quantidade de subscrições adquiridas.

II – No caso do serviço referente ao item 7 da tabela constante do Anexo I

a) **provisoriamente**, provisoriamente, pelo responsável pelo acompanhamento e fiscalização do contrato, mediante termo detalhado, após verificação do cumprimento das exigências de caráter técnico, na data da conclusão do treinamento;

b) **definitivamente**, no prazo de 5 (cinco) dias úteis, contados do recebimento provisório, pelo servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências descritas no item 3.13 do Anexo I.

III – No caso do serviço referente ao item 8 da tabela constante do Anexo I

a) **provisoriamente**, pelo responsável pelo acompanhamento e fiscalização do contrato, mediante termo detalhado, após verificação do cumprimento das exigências de caráter técnico, na data de conclusão da fase de Implantação, Configuração e Ativação da solução;

b) **definitivamente**, no prazo de 10 (dez) dias úteis, contados do recebimento provisório, pelo servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências descritas no item 4.11 do Anexo I.

IV – No caso dos serviços referentes aos itens 9 a 13 da tabela constante do Anexo I

a) **provisoriamente**, provisoriamente, pelo responsável pelo acompanhamento e fiscalização do contrato, mediante termo detalhado, após verificação do cumprimento das exigências de caráter técnico, na data da entrega e apresentação dos relatórios indicados no item 5.17 do Anexo I;

b) **definitivamente**, no prazo de 10 (dez) dias úteis, contados do recebimento

provisório, pelo servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

Parágrafo Primeiro: Se, após o recebimento provisório, constatar-se que os serviços foram prestados em desacordo com a proposta, com defeito, fora de especificação ou incompletos, após a notificação por escrito à **CONTRATADA**, serão interrompidos os prazos de recebimento e suspenso o pagamento, até que sanada a situação.

Parágrafo Segundo: A **CONTRATADA** terá o prazo de 5 (cinco) dias úteis para sanear as irregularidades detectadas, exceto para irregularidades referentes ao serviço de implantação da solução proposta (item 8 da tabela do Anexo I), caso em que o prazo será de 10 (dez) dias úteis, sob pena da aplicação de multa prevista neste instrumento.

Parágrafo Terceiro: O objeto da contratação poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

Parágrafo Quarto: O recebimento provisório ou definitivo não excluirá a responsabilidade civil nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

CLÁUSULA QUINZE: DA EXTINÇÃO DO CONTRATO

O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

Parágrafo Primeiro: O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o **CONTRATANTE**, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

Parágrafo Segundo: A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da **CONTRATADA** pelo **CONTRATANTE** nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

Parágrafo Terceiro: Caso a notificação da não-continuidade do contrato de que trata o parágrafo anterior ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

Parágrafo Quarto: O contrato pode ainda ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

Parágrafo Quinto: Na hipótese do parágrafo anterior, aplicam-se também os artigos 138 e 139 da mesma Lei.

Parágrafo Sexto: A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

Parágrafo Sétimo: Se a operação implicar mudança da pessoa jurídica **CONTRATADA**, deverá ser formalizado termo aditivo para alteração subjetiva.

Parágrafo Oitavo: O termo de rescisão, sempre que possível, será precedido:

I. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

II. Relação dos pagamentos já efetuados e ainda devidos;

III. Indenizações e multas.

CLÁUSULA DEZESSEIS: DA DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta dos recursos orçamentários consignados a este Regional na Lei Orçamentária nº 14.822, de 22 de janeiro de 2024, publicada no D.O.U. em 23/01/2024, conforme Programa de Trabalho 15.103.02.122.0033.4256.0035 e Natureza da Despesa 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação - PJ, e nos exercícios subsequentes, à conta da dotação orçamentária que atenda despesas da mesma natureza.

CLÁUSULA DEZESSETE: DOS CASOS OMISSOS

Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei nº 14.133/2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DEZOITO: DAS ALTERAÇÕES CONTRATUAIS

Este contrato poderá ser alterado conforme art. 124 e art. 125 da Lei nº 14.133/2021, por meio de termo aditivo, exceto na ocorrência de registros que não caracterizam alteração dos contratos, que poderão ser realizados por apostilamento, conforme art. 136 e incisos da Lei nº 14.133/2021.

Parágrafo Primeiro: A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

Parágrafo Segundo: A formalização do termo aditivo é condição para a execução, pela **CONTRATADA**, das prestações determinadas pelo **CONTRATANTE** no curso da execução do contrato, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização deverá ocorrer no prazo máximo de 1 (um) mês.

CLÁUSULA DEZENOVE: DA PUBLICAÇÃO

Incumbirá ao **CONTRATANTE** providenciar a publicação deste instrumento e seus aditamentos no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA VINTE: DO FORO

O Foro para solucionar os litígios que decorrerem da execução deste contrato, e que não puderem ser compostos por meios alternativos de prevenção e resolução de controvérsias, será o da Seção Judiciária de São Paulo/SP da Justiça Federal, conforme art. 92, §1º, da Lei nº 14.133/21.

Para firmeza e validade do pactuado, os contraentes assinam o presente contrato.

São Paulo, data da última assinatura eletrônica.

Assinado digitalmente
VALDIR FLORINDO
Desembargador Presidente do Tribunal

Assinado digitalmente
JOSÉ ANDRÉ MENDES COIMBRA
Consórcio Petaservice Sec.

TESTEMUNHAS:

Assinado digitalmente
CLAUDIA SANT'ANNA PINHEIRO
Diretora da Coordenadoria de Segurança de TIC

Assinado digitalmente
MARCIO NISI GONÇALVES
Diretor da Secretaria de Tecnologia da Informação e Comunicações

ANEXO I

ESPECIFICAÇÃO DO OBJETO

1. OBJETO

Registros de preços visando a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução proposta, pelo período de 24 (vinte e quatro) meses, conforme a tabela seguinte:

GRUPO 1 (G1)					
Item	**Descrição**	**Faixa**	**Faixa de subscrição por ativo**	**Unidade de medida**	**Quantidade**
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	1
2		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	19.799
3		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	30.796
4		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	42.152
5		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10.846
6		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	38
7	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes	Serviço pontual, por turma de treinamento	37
8	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25
9	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1
10		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	12
11		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	9
12		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	7
13		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1

1.1. Definições para fins desta especificação:

1.1.1. Define-se “Ativo monitorado” como sendo uma estação de trabalho, notebook, dispositivo móvel, servidor, container, firewall, ativo de rede ou qualquer equipamento similar ao listado que possua endereço IP próprio e distinto e que deverá ser monitorado pela solução proposta. Poderá

ser físico ou virtual e poderá estar hospedado em ambiente local (on-premise) ou em nuvem.

1.1.1.1. Relativo a container, deverá ser contabilizado como "Ativo monitorado" o host que hospeda o(s) container(s), para efeito de subscrição.

1.1.1.2. Caso o ativo possua mais de um endereço IP, será contabilizado um único "Ativo monitorado" para efeito de subscrição.

1.1.2. Define-se "Tráfego diário monitorado" como sendo volume médio diário do tráfego da rede interna (em Gbps - Gigabits por segundo) que deverá ser monitorado pela solução proposta.

1.1.3. Para os dados do ambiente do CONTRATANTE que serão coletados pela solução proposta, compreende-se as seguintes definições:

1.1.3.1. "Dados de logs", "logs de evento" ou simplesmente "log": informações produzidas sobre eventos ocorridos nos sistemas operacionais, aplicações, servidores, endpoints, ativos de rede ou outros componentes do ambiente computacional.

1.1.3.2. "Dados de telemetria": informações produzidas pelos agentes a serem instalados nos ativos monitorados (quando a solução fizer uso de agentes).

1.1.3.3. "Dados de rede": informações sobre o tráfego de rede.

1.2. Para soluções cuja subscrição seja baseada em EPS (Eventos Por Segundo), a CONTRATADA deve licenciar a solução para uma quantidade mínima de EPS suficiente para atender 100% dos ativos do CONTRATANTE e garantir a escalabilidade da solução, independentemente da quantidade de EPS gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de EPS igual a 8 vezes a referida quantidade de ativos monitorados.

1.2.1. A CONTRATADA deverá aferir mensalmente o consumo de EPS e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para o CONTRATANTE.

1.3. Para soluções cuja subscrição seja baseada em volumetria de logs, a CONTRATADA deve licenciar a solução para uma quantidade mínima de Área de Armazenamento em modalidade SaaS, suficiente para atender 100% dos ativos do CONTRATANTE e garantir a escalabilidade da solução, independentemente do volume de logs, dados de telemetria e de rede gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de GB (gigabytes) igual a 2 vezes a referida quantidade de ativos monitorados e a retenção dos logs estipulada no item 2.8.

1.3.1. A CONTRATADA deverá aferir mensalmente a volumetria e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções

no quantitativo se necessário, sem custo para o CONTRATANTE.

1.3.2. Define-se "Área de Armazenamento" como sendo a área disponibilizada por meio da solução contratada para armazenamento dos logs em ambiente SaaS, coletados pela solução.

2. <u>GRUPO 1 (G1) - ITENS 1 A 6</u> – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

2.1. A solução contratada visa o monitoramento contínuo e ininterrupto dos ativos computacionais do CONTRATANTE (supramencionados como "Ativos monitorados") por meio das etapas de, mas não se limitando à, coleta, processamento e correlação de logs de eventos, dados de telemetria e/ou de rede de tais ativos, com o objetivo de, após análise contextualizada das etapas mencionadas, identificar eventos suspeitos ou incomuns, direcionados ao CONTRATANTE.

2.2. A solução deve possuir as características mínimas constantes nesta especificação, devendo ser constituída de softwares, licenças, subscrições e garantias, de tal forma que haja a total compatibilidade entre seus componentes.

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos do CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity Behavior Analytics). Neste caso, entende-se por "Aplicações" como sendo os softwares instalados nos ativos monitorados.

2.5. A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais do CONTRATANTE, compreendendo:

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pelo CONTRATANTE;

2.5.2. Registrar e comunicar os incidentes de segurança cibernética para o CONTRATANTE, com as respectivas recomendações para tratamento e mitigação das ameaças, conforme especificação técnica contida neste documento;

2.5.3. Elaborar procedimentos padronizados contendo as melhores práticas para tratamento e resposta dos incidentes confirmados, que serão posteriormente executados pelas equipes responsáveis do CONTRATANTE;

2.5.4. Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para o CONTRATANTE.

2.5.4.1. O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.

2.5.4.1.1. O módulo ou ferramenta deve ser capaz de, minimamente:

a. Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:

a.1. Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;

a.2. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

a.3. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;

a.4. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;

a.5. Permitir inserir evidências coletadas de eventual análise forense de

host e rede como um complemento da análise do incidente;

a.6. Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;

a.7. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

b. Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:

b.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;

b.2. Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;

b.3. Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.

c. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados.

c.1. Os relatórios gerados deverão ser encaminhados para o CONTRATANTE.

2.5.4.1.2. O módulo ou ferramenta de ITSM deverá estar licenciado para o CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegida por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.

2.6. A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes *on-premises* e em nuvem, a fim de realizar a implantação distribuída da arquitetura.

2.6.1. O fabricante da solução proposta para monitoramento, detecção, notificação, investigação

e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;

2.6.2. Deve ter instância própria para cada CONTRATANTE, isto é, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

2.6.3. Todas as licenças e subscrições necessárias para o pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA, conforme as quantidades e faixas discriminadas nesta especificação.

2.6.4. Coletores de logs: o software dos coletores de logs, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes eventualmente necessários para a coleta e centralização de logs de eventos e/ou dados de telemetria deverão ser fornecidos pela CONTRATADA, podendo ser de fabricantes distintos da solução.

2.6.5. Coletores de tráfego de rede: o software dos coletores de tráfego de rede, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes (de software ou hardware) eventualmente necessários para a coleta e centralização de dados de tráfego de rede deverão ser fornecidos pela CONTRATADA, podendo ser de fabricantes distintos da solução, devendo ser compatíveis com a infraestrutura do CONTRATANTE (interfaces de rede de 1Gbps e 10Gbps).

2.6.5.1. O tráfego de rede deverá ser mensurado de acordo com o ambiente do CONTRATANTE.

2.6.6. O CONTRATANTE disponibilizará, no máximo, os seguintes recursos em ambiente virtual a serem usados pelos coletores de logs e de tráfego de rede (os recursos podem ser distribuídos entre diversas máquinas virtuais - uma para cada coletor, se necessário):

2.6.6.1. 12 vCPUs;

2.6.6.2. 32Gb vRAM;

2.6.6.3. 200GB de espaço em disco.

2.6.7. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pelo CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pelo CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério do CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais para o CONTRATANTE, a entrega da infraestrutura (total ou

remanescente) e em conformidade com a estrutura computacional do CONTRATANTE.

2.6.8. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de ataques nos *endpoints*, coletando informações *on-line* do sistema, incluindo informações básicas de identificação de ativos, processos em execução, logs e outros dados de telemetria e as enviando de volta à solução para análise.

2.6.9. O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:

2.6.9.1. Google Chrome;

2.6.9.2. Mozilla Firefox.

2.6.10. O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.6.10.1. Caso a solução seja composta por diversas ferramentas, a console de gerência principal deve permitir a visibilidade integrada e total do monitoramento, detecção, notificação, investigação e resposta aos ataques cibernéticos detectados e sendo tratados em todo o ambiente computacional.

2.6.10.2. As demais ferramentas podem estar hospedadas em ambiente provisionado pela CONTRATADA, sem custos adicionais para o CONTRATANTE.

2.6.10.3. Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.

2.6.11. O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados ou para a quantidade de eventos por segundo (conforme item 1.2) ou para o volume de armazenamento de logs em ambiente SaaS (conforme item 1.3) de forma a abranger o escopo completo de ativos do CONTRATANTE, conforme conceito apresentado nesta especificação técnica. Assim, é obrigatório que a solução cubra 100% do ambiente do CONTRATANTE, incluindo estações de trabalho, notebooks, dispositivos móveis, servidores físicos e virtuais, containers, firewalls, ativos de rede ou qualquer equipamento similar ao listado, e não somente parcialmente, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.

2.7.1. A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do

licenciado em até 30%.

2.7.1.1. Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.

2.8. A solução deve possuir retenção mínima de 3 (três) meses de registros prontamente acessíveis ("Logs Quentes"). Após este período, a solução deve suportar, no mínimo, 9 (nove) meses de registros arquivados ("Logs Frios") - totalizando 12 (doze) meses de registros - bem como permitir a exportação destes logs/dados de telemetria/de rede para armazenamento em ambiente de propriedade do CONTRATANTE.

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 6 (seis) meses.

2.8.2. Deve haver a opção de exportação de logs/dados de telemetria/de rede em formato aberto (plain text) podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins.

2.8.3. A solução não deve possuir mecanismos que limitem ou onerem o CONTRATANTE com base na quantidade/volume de dados a serem exportados.

2.9. A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do Open LDAP, monitorando diferentes vetores de ataque, como:

2.9.1. Movimentação lateral com uso de credenciais locais de máquina;

2.9.2. Ataques de força bruta em contas locais de máquinas;

2.9.3. Usuários locais que tentam apagar arquivos de evento dos registros da máquina.

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

2.9.4.3. Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;

2.10. A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.

2.11. A solução deve monitorar qualquer tipo de acesso de usuário:

2.11.1. Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução ou de terceiros;

2.11.2. Com credenciais do domínio – monitoramento do Microsoft Active Directory;

2.11.3. Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;

2.11.3.1. Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso – minimamente data, hora e IP.

2.12. A solução deve suportar IPv4 ou IPv4/IPv6.

2.13. Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);

2.13.4. Web filtering;

2.13.5. Antivírus;

2.13.6. Microsoft Active Directory;

2.13.7. Open LDAP;

2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);

2.13.9. Servidores HTTP (HTTP Servers);

2.13.10. Balanceadores de Carga (Load Balancers);

2.13.11. DNS;

2.13.12. DHCP;

2.13.13. ELK Stack;

2.13.14. Sistemas Operacionais.

2.14. A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.

2.14.1. A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores

nativos.

2.14.2. A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.

2.14.2.1. A solução deve permitir utilização de expressões regulares (regex) nos parsers.

2.14.2.2. A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.

2.15. A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:

2.16.1. Sistemas com maior atividade baseada em volume de tráfego;

2.16.2. Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;

2.16.3. Atividades de rede baseada em porta de destino e endereços de origem e destino;

2.16.4. Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.

2.16.5. Servidores DNS em uso;

2.16.6. Relação das principais aplicações em uso na rede;

2.16.7. Identificação de picos de consumo de banda de acesso à rede;

2.16.8. Relação de dispositivos, servidores e serviços que operam na rede.

2.17. A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente do CONTRATANTE:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):

2.17.1.1. Checkpoint para proteção de perímetro (Firewall);

2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);

2.17.1.3. Forcepoint para proteção de perímetro (Firewall);

2.17.1.4. Microsoft Active Directory para serviços de diretório.

2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:

2.17.2.1. Open LDAP para serviços de diretório;

2.17.2.2. OpenVPN;

2.17.2.3. Citrix;

2.17.2.4. RDP e RDPWeb;

2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;

2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado

2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;

2.17.2.8. Keycloak para gerenciamento de identidade e acesso;

2.17.2.9. midPoint para segurança de identidades (identity security);

2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);

2.17.2.11. Loqed;

2.17.2.12. Varonis;

2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;

2.17.2.14. Kaspersky para proteção de endpoint;

2.17.2.15. Blackberry Cylance para proteção de endpoint.

2.17.2.16. Check Point Harmony para proteção de endpoint;

2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);

2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;

2.17.2.19. Tenable.ad para proteção do Active Directory;

2.17.2.20. Trivy para varredura de vulnerabilidades;

2.17.2.21. VMware/vCenter para virtualização de máquinas;

2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;

2.17.2.23. Hyper-V para virtualização de máquinas;

2.17.2.24. Ovirt para virtualização de máquinas;

2.17.2.25. Docker e Kubernetes;

2.17.2.26. Apache HTTP Server;

2.17.2.27. HAProxy;

2.17.2.28. Ingress;

2.17.2.29. Nginx;

2.17.2.30. Switches Cisco MDS;

2.17.2.31. Switches H3C;

2.17.2.32. Switches HP;

2.17.2.33. Switches Huawei;

2.17.2.34. Roteadores Cisco;

2.17.2.35. Roteadores Juniper;

2.17.2.36. Roteadores MikroTik;

2.17.2.37. Access Points Aruba;

2.17.2.38. Access Points Ruckus;

2.17.2.39. Controladoras Virtuais Aruba;

2.17.2.40. Bacula para serviços de backup;

2.17.2.41. Commvault (software de backup);

2.17.2.42. Veeam (software de backup);

2.17.2.43. Storage Huawei;

2.17.2.44. Storage IBM;

2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;

2.17.2.46. Dell EMC Data Domain;

2.17.2.47. Dell EMC Isilon.

2.18. A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:

2.18.1. De forma nativa (sem a necessidade de customização de parsers):

2.18.1.1. AWS CloudTrail, via SQS ou API;

2.18.1.2. Google Cloud Platform, via API;

2.18.1.3. Google Workspace/Google Apps, via API;

2.18.1.4. Microsoft Office 365, via API.

2.19. A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.

2.19.1. De forma nativa (sem a necessidade de customização de parsers):

2.19.1.1. Windows 7;

2.19.1.2. Windows 8.1;

2.19.1.3. Windows 10;

2.19.1.4. Windows 11;

2.19.1.5. Windows Server 2008 R2;

2.19.1.6. Windows Server 2012;

2.19.1.7. Windows Server 2012 R2;

2.19.1.8. Windows Server 2016;

2.19.1.9. Windows Server 2019;

2.19.1.10. Windows Server 2022;

2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;

2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;

2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;

2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;

2.19.1.15. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;

2.19.1.16. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;

2.19.1.17. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;

2.19.1.18. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;

2.19.1.19. Amazon Linux;

2.19.1.20. Debian Linux;

2.19.1.21. Ubuntu Linux.

2.20. Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo

ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico do CONTRATANTE.

2.21. A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.

2.22. A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.

2.23. A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.

2.24. A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:

2.24.1. Requisição a domínio suspeito;

2.24.2. Execução de processos suspeitos;

2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);

2.24.4. Comunicação com servidores Command & Control;

2.24.5. Tentativa de desabilitar recursos de Sysmon;

2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;

2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;

2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;

2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;

2.24.10. Detecção de execução do Mimikatz e variações;

2.24.11. Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;

2.24.12. Detecção de tentativas de criação de reverse shells para Command & Control.

2.25. A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC's (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).

2.26. A solução deve possuir listas de terceiros com informações de IoC's com, no mínimo, IPs,

domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.27. A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.28. A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.

2.29. A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).

2.30. A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.

2.30.1. A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.

2.30.2. Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional do CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.

2.30.3. Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.

2.31. A solução deve possuir nativamente a capacidade de "deception" ou permitir que se implemente capacidade similar por meio de ferramenta complementar e integrada a solução proposta, possibilitando a marcação de ativos, credenciais, usuários e arquivos específicos como sendo "iscas" a fim de, quando acessados, gerarem alertas, facilitando o monitoramento e auditoria contínuos.

2.31.1. Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 5 (cinco) máquinas no ambiente;

2.31.1.1. Os honeypots devem ser fornecidos em formato OVA – virtual appliance.

2.31.2. Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;

2.31.3. Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;

2.31.4. Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.

2.31.5. A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).

2.32. Quando a solução não possuir capacidade de "deception", a capacidade de "Breach and Attack Simulation" (BAS) pode ser apresentada, com os seguintes critérios mínimos:

2.32.1. Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 3 (três) tipos de licenças devem estar incluídas sem custos adicionais para o CONTRATANTE;

2.32.2. Deve ser executado, pelo menos, mensalmente;

2.32.3. Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional do CONTRATANTE;

2.32.4. As simulações devem utilizar diferentes vetores de ataque;

2.32.5. O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.

2.33. A solução que fizer uso de agentes deve permitir sua instalação de forma "silenciosa" nos ativos a serem monitorados.

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.

2.35. A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.

2.36. Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.

2.37. Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.

2.38. Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.

2.39. Os agentes e coletores devem enviar os dados para o console de maneira:

2.39.1. Segura e criptografada;

2.39.2. Que não haja impacto na performance ou disponibilidade da rede do CONTRATANTE.

2.40. Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede do CONTRATANTE.

2.41. A solução deve monitorar, no mínimo:

2.41.1. Força bruta no ativo (brute force – asset);

2.41.2. Força bruta em conta local (brute force – local account);

2.41.3. Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);

2.41.4. Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);

2.41.5. Correspondência de Threat Intel (endpoint threat intelligence match);

2.41.6. Exploração mitigada (exploit mitigated);

2.41.7. Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;

2.41.8. Processo sinalizado no ativo (flagged process on asset);

2.41.9. Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);

2.41.10. Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local credentials);

2.41.12. Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);

2.41.13. Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;

2.41.14. Criação de nova conta de usuário local (new local user account created);

2.42. A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.

2.43. A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no

ambiente computacional do CONTRATANTE e que não estejam sendo monitorados.

2.44. A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.

2.44.1. A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.

2.45. A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:

2.45.1. Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;

2.45.2. Identificar quais eventos devem gerar alertas;

2.45.3. A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.

2.46. O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.47. A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.

2.48. A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.

2.49. A solução deve prover funcionalidade de detecção de padrões em eventos coletados:

2.49.1. A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;

2.50. A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.

2.51. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

2.52. A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

2.53. A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.

2.53.1. Essas informações podem ser disponibilizadas por interação humana após investigação.

2.54. A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.

2.55. A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.

2.56. A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.

2.56.1. A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.

2.57. A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.

2.58. A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.

2.58.1. Nativamente, para os seguintes formatos de arquivos, no mínimo:

2.58.1.1. .bat

2.58.1.2. .cfg

2.58.1.3. .conf

2.58.1.4. .config

2.58.1.5. .dll

2.58.1.6. .exe

2.58.1.7. .ini

2.58.1.8. .sys

2.58.2. A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.

2.59. Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.

2.60. A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps do CONTRATANTE e realizar a análise dos dados coletados.

2.61. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

2.61.1. A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré-definidas.

2.61.1.1. No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.

2.62. A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:

2.62.1. Envio de e-mails.

2.62.2. Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:

2.62.2.1. Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;

2.62.2.2. Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;

2.62.3. Com integrações para as soluções nativas indicadas no item 2.17.1:

2.62.3.1. Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;

2.62.3.2. Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.

2.62.4. A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:

2.62.4.1. Ser totalmente automática;

2.62.4.2. Aguardar uma interação humana para ser realizada.

2.63. Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.

2.64. A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.

2.65. A solução deve possuir módulo de investigação e detecção integrados.

2.66. A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.

2.67. A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.

2.67.1. As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para o CONTRATANTE, para viabilizar sua integração.

2.68. A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.

2.69. A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.

2.70. A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.

2.71. A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.

2.71.1. A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.

2.72. A solução deve ser capaz de classificar a relevância dos eventos, minimamente, em “crítico”, “alto”, “médio” e “baixo”.

2.73. A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.

2.74. A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.

2.75. A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.

2.75.1. Deve ser possível ativar ou desativar qualquer modelo de detecção.

2.75.2. A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para o CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.

2.76. A solução deve permitir a criação de listas de exceção de objetos para redução de falsos-positivos.

2.77. A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.

2.78. A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.

2.79. A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;

2.80. A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.

2.81. A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.

2.81.1. A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.

2.82. A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

2.83. A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.

2.84. A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.

2.84.1. Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

2.85. A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.

2.86. A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.

2.87. A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos

utilizados para futuras consultas.

2.88. A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.

2.88.1. Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas do CONTRATANTE.

2.88.2. Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.

2.88.3. Deve possuir dashboards pré-configurados que permitam a visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.

2.88.4. Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:

2.88.4.1. Alertas e incidentes mais frequentes;

2.88.4.2. Nível de risco do ambiente;

2.88.4.3. Relatório dos últimos 30 (trinta) dias da detecção de incidentes;

2.88.4.4. Top 10 (dez) ativos com incidentes;

2.88.4.5. Os ativos que mais sofreram incidentes em um determinado período;

2.88.4.6. Os usuários que mais sofreram incidentes em um determinado período;

2.88.4.7. Ativos e contas descobertas;

2.88.4.8. Ameaças descobertas e classificadas conforme a cadeia de ataque.

2.88.5. Deve permitir configuração de atualização do tempo de cada dashboard.

2.88.6. Deve permitir exportação dos relatórios para os seguintes formatos:

2.88.6.1. Planilha: CSV e/ou Excel;

2.88.6.2. Texto: HTML e/ou PDF.

2.89. A solução deve permitir o gerenciamento de usuários, funções e permissões.

2.90. A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.

2.91. A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do

console.

2.92. A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.

2.93. A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.94. A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.94.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas ao CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.94.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 6 (seis) domínios DNS do CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.94.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.94.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.94.4.1. Na Darknet;

2.94.4.2. Em plataformas de compartilhamento de documentos;

2.94.4.3. Pelas seguintes categorias:

2.94.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.94.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.94.4.3.3. Por Geolocalização.

2.94.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos

considerando, no mínimo, as seguintes categorias:

2.94.5.1. Domínio DNS;

2.94.5.2. Endereço de e-mail;

2.94.5.3. Endereço Bitcoin;

2.94.5.4. Endereço Ethereum;

2.94.5.5. Endereço MAC;

2.94.5.6. Hash IPFS;

2.94.5.7. IBAN (Número de Conta Bancária Internacional);

2.94.5.8. IP e CIDR;

2.94.5.9. Número de telefone;

2.94.5.10. Número do cartão de crédito;

2.94.5.11. URL.

2.94.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.

2.94.7. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 (um) ano.

2.94.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

2.94.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.94.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.94.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.94.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.94.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.94.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.94.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações

sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis do CONTRATANTE.

2.94.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.94.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.94.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.94.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.94.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;

2.94.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.94.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.94.10.4. Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;

2.94.10.5. Investigação de origens de vazamentos de, no mínimo:

2.94.10.5.1. Grupos de hackers;

2.94.10.5.2. Ameaças em fóruns;

2.94.10.5.3. Salas de chats reservadas;

2.94.10.5.4. Carteira de bitcoins e endereços;

2.94.10.5.5. Registros históricos.

2.94.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.94.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.95. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

PAGAMENTO

2.96. A emissão do termo de recebimento provisório será feita após a instalação e configuração do console de gerência, dos coletores de logs, dos coletores de tráfego de rede e de agentes em estações de trabalho e em servidores.

2.97. As subscrições deverão ser fornecidas conforme a quantidade de ativos definida pelo CONTRATANTE e deverão ser nomeadas (para cada CONTRATANTE). A comprovação do fornecimento se dará através da Nota Fiscal e o pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação às subscrições efetivamente fornecidas em nome do CONTRATANTE, conforme volumetria mínima prevista.

2.98. A emissão do termo de recebimento definitivo será feita após a verificação do perfeito funcionamento do console de gerência, dos coletores de logs, dos coletores de tráfego de rede, de agentes em estações de trabalho, de agentes em servidores e da integração de todos os componentes.

2.99. A quantidade de agentes a serem considerados em cada tipo de ativo nos termos de recebimento provisório e definitivo deve ser acordada na fase de Planejamento e Projeto (item 4.4.1), não sendo superior a 10% do parque computacional do CONTRATANTE.

2.100. A distribuição dos agentes (no restante do parque computacional) para os outros ativos a serem monitorados será de responsabilidade do CONTRATANTE, sem prejuízo do suporte que a CONTRATADA deve fornecer para a realização dessa etapa.

2.101. O pagamento da subscrição deve ser anual, em parcela única, sendo realizado somente após a emissão do termo de recebimento definitivo.

3. <u>GRUPO 1 (G1) - ITEM 7</u> – Requisitos mínimos de treinamento na solução

3.1. A CONTRATADA deve oferecer treinamento contemplando a perfeita instalação, configuração, operação e utilização da solução contratada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;

3.2.5. Configurar honeypots, quando a solução tiver essa capacidade;

3.2.6. Configurar serviço de Breach and Attack Simulation (item 2.32), quando a solução tiver essa capacidade;

3.2.7. Configurar regras;

3.2.8. Configurar alertas;

3.2.9. Configurar playbooks;

3.2.10. Investigar incidentes;

3.2.11. Pesquisar em logs;

3.2.12. Criar dashboards;

3.2.13. Criar relatórios e agendamento de relatórios;

3.2.14. Gerenciar usuários, funções e permissões;

3.2.15. Identificar as possíveis causas de problemas e atuar na sua resolução;

3.2.16. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);

3.2.17. Conhecer os procedimentos para abertura de chamados técnicos;

3.2.18. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. Devem ser fornecidos todos os recursos necessários para a realização do treinamento (material didático, equipamentos, instrutor, etc.). Os treinamentos serão realizados nas dependências do CONTRATANTE ou na modalidade EAD, a critério do CONTRATANTE.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. O treinamento deve ser o treinamento oficial do fabricante ou com material oficial do fabricante.

3.6. O material didático e demais documentações deverão ser fornecidos, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.7. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades do CONTRATANTE.

3.8. O treinamento deverá ser ministrado com carga horária mínima de 40 (quarenta) horas, com fornecimento de certificados a todos os participantes, em papel timbrado da empresa, constando:

nome do treinando, identificação do treinamento, carga horária, período de ocorrência e conteúdo programático.

3.9. A critério do CONTRATANTE, o treinamento poderá ser dividido em turmas de, no mínimo, 2 (dois) alunos e, no máximo, 8 (oito) alunos.

3.10. O treinamento deverá ser ministrado em horário definido pelo CONTRATANTE, em dias úteis.

3.11. O cronograma do treinamento será definido em conjunto com o CONTRATANTE, na fase de Planejamento e Projeto (item 4.4.1).

PAGAMENTO

3.12. A emissão do termo de recebimento provisório do treinamento será feita após a conclusão do treinamento.

3.13. A emissão do termo de recebimento definitivo do treinamento será feita após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário o CONTRATANTE poderá solicitar a realização de novo treinamento com a reformulação que achar necessária.

3.14. O pagamento do treinamento deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

4. <u>GRUPO 1 (G1) - ITEM 8</u> – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 45 (quarenta e cinco) dias corridos contados a partir da assinatura do contrato, quando serão executados o planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

4.2. As atividades que propiciarão criar, alterar e manter controles de segurança cibernética, além de medir a eficiência e eficácia dos serviços de SOC quanto à sua utilização dentro do negócio, serão adequadas nesta fase de ativação do contrato, conforme parâmetros (baseline) a serem acordados

entre as partes.

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional do CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs e dos coletores de tráfego de rede;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1);

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal

funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:

4.4.3.5.1. Base de incidentes em aberto (em tratamento);

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução (item 4.4.5), realizar a configuração para o correto funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

RESPONSABILIDADES DA CONTRATADA

4.6. São responsabilidades da CONTRATADA:

4.6.1. Prestar os serviços conforme previsto e delimitado por esta especificação, dentro das normas e especificações técnicas aplicáveis à espécie;

4.6.2. Respeitar as normas e regulamentos do CONTRATANTE, inclusive aqueles relativos ao acesso, permanência e trânsito de pessoas e materiais, no estabelecimento desta, as quais deverão lhe ser fornecidas previamente e por escrito;

4.6.3. Observar integralmente a legislação e normas infralegais aplicáveis aos serviços, inclusive aqueles referentes à segurança cibernética e medicina do trabalho;

4.6.4. Zelar pela disponibilidade da infraestrutura de TI do CONTRATANTE durante a realização

dos serviços propostos;

4.6.5. Realizar a manutenção de software e hardware de sua propriedade e utilizados para a prestação dos serviços propostos.

4.7. A implantação, configuração, ativação e atualização da solução será de responsabilidade da CONTRATADA, bem como as despesas diretas ou indiretas para a execução das atividades pela sua equipe técnica.

4.8. A instalação e atualização dos softwares nos ativos monitorados (item 1.1.1) poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pelo CONTRATANTE.

4.9. O processo de implantação, configuração, ativação e atualização da solução deverá ser realizado por técnicos capacitados da CONTRATADA, acompanhados por servidores do CONTRATANTE.

PAGAMENTO

4.10. A emissão do termo de recebimento provisório será feita após a conclusão da fase de Implantação, Configuração e Ativação da solução (item 4.4.2);

4.11. A emissão do termo de recebimento definitivo será feita após a conclusão da fase de Definição de Processos e Outras Configurações (item 4.4.3);

4.12. O pagamento do serviço de implantação deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

5. <u>GRUPO 1 (G1) - ITENS 9 A 13</u> – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.1.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações do CONTRATANTE.

5.1.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste edital.

5.1.3. A solução contratada deve ter instância própria para o CONTRATANTE, exclusiva e

dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.1.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.1.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.1.5.1. Assegurar de que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.1.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

5.1.5.3. Desenvolver atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.1.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.2. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar o CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.3. Os incidentes de segurança cibernética são os relacionados aos eventos de segurança dos ativos monitorados como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento pela solução proposta e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações do CONTRATANTE.

5.4. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.5. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for

submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança deste CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.6. O CONTRATANTE deverá ser informado sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.7. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pelo CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.8. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.9. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.10. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

5.10.1. Ativação e configuração dos módulos contratados;

5.10.2. Integração dos componentes contratados com o ambiente do CONTRATANTE;

5.10.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.10.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.10.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.10.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.10.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pelo CONTRATANTE;

5.10.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pelo CONTRATANTE;

5.10.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.10.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.10.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.10.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.10.13. Configuração de fontes de eventos;

5.10.14. Configuração de usuários VIP e usuários de serviço;

5.10.15. Criação de alertas customizados;

5.10.16. Configuração de coletores de eventos;

5.10.17. Configuração de monitoramento de arquivos e diretórios;

5.10.18. Liberação de acesso à solução para usuários autorizados pelo CONTRATANTE;

5.10.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);

5.10.20. Zelar e empregar todos os esforços necessários para garantir o atendimento ao SLA estabelecido neste edital, tanto que se refere aos serviços quanto às soluções contratadas;

5.10.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pelo CONTRATANTE;

5.10.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.11. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética do CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.11.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

5.11.2. Fazer uma reunião semanal com a equipe do CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério do CONTRATANTE).

5.11.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica

contida neste documento (item 5.17);

5.11.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;

5.11.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 9 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.12. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.12.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.12.2. Criar, em colaboração com a equipe de segurança cibernética do CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.12.3. Revisar, sempre que necessário e/ou solicitados pelo CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.12.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.13. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.13.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.13.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.13.3. O serviço deve poder ser executado sob demanda.

5.13.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.14. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.14.1. Monitorar equipamentos e softwares componentes das soluções de segurança do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.14.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.14.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 (vinte e quatro) horas.

5.14.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente do CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 (dois) dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.14.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e confidencialidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados do CONTRATANTE foram criptografados. Caso um evento seja classificado como "Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.14.3. Comunicar, à equipe de segurança cibernética do CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.14.4. Informar ao CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.14.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações ao CONTRATANTE:

5.14.5.1. Alertas e notificações;

5.14.5.2. Quantidade de incidentes por categoria;

5.14.5.3. Quantidade de incidentes por criticidade (severidade);

5.14.5.4. Quantidade de incidentes que geraram crise;

5.14.5.5. Porcentagem dos incidentes originários do monitoramento;

5.14.5.6. Quantidade de incidentes tratados/fechados;

5.14.5.7. Quantidade de incidentes registrados.

5.14.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

5.14.6.1. Monitoramento e envio de notificações para a equipe técnica do CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.14.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.14.6.3. Envio de um relatório ao fim do mês ao CONTRATANTE contendo, no mínimo, as informações a seguir:

5.14.6.3.1. Vazamento de dados do CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.14.6.3.2. Descrição do ambiente avaliado;

5.14.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.14.6.3.4. Descrição detalhada dos alertas;

5.14.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.14.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.14.6.3.7. Apresentação técnica dos resultados, incluindo o detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.15. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.15.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de

segurança que, após analisados, demonstraram ser um ataque ao ambiente do CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.15.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.15.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

5.15.4. Definir, junto à equipe de segurança cibernética do CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.15.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética do CONTRATANTE.

5.15.5. Apoiar a equipe técnica do CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.15.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.15.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética do CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.15.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la ao CONTRATANTE.

5.15.8.1. Qualquer tipo de alteração no parque computacional do CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pelo próprio CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.15.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.15.9.1. A necessidade de análise forense será indicada pelo CONTRATANTE, seguindo

os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.15.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.15.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pelo CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.15.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.15.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.16. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

PAGAMENTO

5.17. A emissão do termo de recebimento provisório será feita após a entrega e apresentação dos relatórios indicados nesta especificação:

5.17.1. Incidentes de segurança cibernética (item 5.14.5);

5.17.2. Deep/Dark Web (item 5.14.6.3);

5.17.3. Breach and Attack Simulation (item 2.32.5), quando a solução tiver essa capacidade;

5.17.4. SLA (itens 5.22.2 e 5.23.8).

5.18. A emissão do termo de recebimento definitivo será feita após a verificação dos serviços prestados e sua aderência às condições estabelecidas nesta especificação.

5.19. O pagamento do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser mensal, sendo realizado somente após a emissão do termo de

recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período (item 5.24 e subitens) e das multas aplicadas, quando houver.

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.20. Confidencialidade:

5.20.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pelo CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.20.1.1. A CONTRATADA obriga-se a tratar como “segredos comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termos de Confidencialidade conforme anexos VIII e IX;

5.20.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

GARANTIA E ACORDO DE NÍVEL DE SERVIÇO

5.21. Da garantia:

5.21.1. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado.

5.21.2. A solução deve contar com garantia integral do fabricante (Garantia Compreensiva) durante toda a vigência do contrato e deve comportar a garantia comumente utilizada pelo comércio e prevista no Código de Defesa do Consumidor acrescida de suporte técnico nos moldes desta especificação.

5.22. Um acordo de nível de serviço (SLA – Service Level Agreement) define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA.

5.22.1. Tais índices serão medidos e aplicados aos serviços contratados e prestados pela CONTRATADA.

5.22.2. Mensalmente, os dados de nível de serviço devem ser apresentados ao CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

5.22.3. A abrangência e o nível de detalhamento serão definidos conforme as necessidades identificadas pelo CONTRATANTE, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas à CONTRATADA.

5.22.4. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

5.22.4.1. Requisição: solicitação do CONTRATANTE para intervenção preventiva ou corretiva no ambiente gerenciado e nos ativos monitorados (item 1.1.1) e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação à CONTRATADA;

5.22.4.2. Incidentes de segurança: conforme definido nos itens 5.3, 5.4 e 5.5.

5.22.4.3. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição do CONTRATANTE ou dos alertas gerados para o ambiente gerenciado, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, em comum acordo, serão prontamente atendidas.

5.22.4.3.1. Severidade crítica: o serviço está totalmente parado ou inoperante;

5.22.4.3.2. Severidade alta: o serviço está ativo mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

5.22.4.3.3. Severidade média: o serviço está operativo, mas suas funcionalidades são executadas com restrições;

5.22.4.3.4. Severidade baixa: o serviço está operativo e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

5.22.4.3.5. Severidade agendado: o atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

5.22.4.4. Triagem: notificação, da CONTRATADA para o CONTRATANTE, de que está ciente da requisição ou do incidente, conforme itens 5.14.3 e 5.14.4.

5.22.4.5. Resolução: comunicação, da CONTRATADA para o CONTRATANTE, das ações

INICIAIS (podendo incluir soluções paliativas enquanto a CONTRATADA busca a solução definitiva para o incidente ou chamado) a serem executadas para resolução da requisição ou do incidente de segurança, conforme item 5.15.8 e subitens.

5.22.4.5.1. A CONTRATADA deve fornecer, em até 48 (quarenta e oito) horas, o restante das ações (contendo a resolução paliativa ou definitiva) a serem executadas para a resolução do incidente ou chamado.

5.22.4.5.2. Caso seja fornecida uma solução paliativa, a CONTRATADA deve atuar proativamente na busca de uma solução definitiva, fornecendo o acompanhamento e suporte necessários para o CONTRATANTE, inclusive sugerindo a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente ou chamado.

5.22.4.5.3. Devido à natureza dos incidentes de segurança cibernética, a sua efetiva contenção e remediação não contarão para contagem dos tempos de SLA, não eximindo a CONTRATADA de registrar esses tempos no módulo de gestão de incidentes de segurança da solução e ITSM integrado.

5.22.5. Os seguintes SLAs devem ser cumpridos:

Atividade	SLA de atendimento
Triagem da requisição/incidente de segurança[2]	Em até 30 (trinta) minutos
Requisição/Incidentes de severidade crítica	Atuação em até 15 (quinze) minutos e resolução[3] em até 1 (uma) hora.
Requisição/Incidentes de severidade alta	Atuação em até 1 (uma) hora e resolução em até 2 (duas) horas.
Requisição/Incidentes de severidade média	Atuação em até 2 (duas) horas e resolução em até 4 (quatro) horas.
Requisição/Incidentes de severidade baixa	Atuação em até 4 (quatro) horas e resolução em até 12 (doze) horas.
Requisição de severidade agendado	Atuação em até 12 (doze) horas e resolução em até 24 (vinte e quatro) horas.

2 Pode ser considerado como o Tempo Médio de Detecção (Mean Time To Detect - MTTD)

3 Para as atividades de Requisição/Incidentes: pode ser considerado como o Tempo Médio de Resposta (Mean Time To Respond - MTTR)

SUPORTE TÉCNICO

5.23. Suporte Técnico:

5.23.1. A abertura de chamados pelo CONTRATANTE deve poder ser efetuada:

5.23.1.1. Pela plataforma web, em sistema de atendimento da CONTRATADA;

5.23.1.2. Pelo envio de mensagem de correio eletrônico;

5.23.1.3. Por meio do módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4);

5.23.1.4. Por telefone.

5.23.2. O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), conforme SLA apresentado (item 5.22.5).

5.23.3. Todo tipo de comunicação e documentação relacionados aos atendimento de chamados devem ser em Português.

5.23.4. A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 7 dias da semana) do CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

5.23.5. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às soluções de software e hardware (inclusive virtual) dos produtos.

5.23.6. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, garantir o fornecimento e instalação de novas versões, patches e hotfixes (tanto de componentes on-premises quanto em nuvem), análise de dúvidas sobre melhores práticas de configuração, entre outros.

5.23.7. A CONTRATADA deve fornecer, mensalmente, relatório oriundo da ferramenta de ITSM (conforme item 2.5.4.1) indicando os SLAs de cada chamado e incidente registrado na solução.

5.23.8. Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deve fornecer, mensalmente, relatório gerencial de serviços, apresentando-o ao CONTRATANTE até o quinto dia útil do mês subsequente ao da prestação do serviço, sendo que devem constar, entre outras

informações, os indicadores/metas de níveis de serviço alcançados conforme item 5.22.5, recomendações técnicas, as solicitações de abonos com justificativa e demais informações relevantes para a gestão contratual, em conformidade aos acordos realizados na fase de Planejamento e Projeto (item 4.4.1).

INDICADORES DE DESEMPENHO E GLOSAS

5.24. Glosa quando a CONTRATADA não produzir os resultados, ou não executar com a qualidade mínima exigida as atividades contratadas, conforme disposto nos indicadores de níveis de serviço.

5.24.1. Para fins de faturamento, o valor mensal da prestação do serviço será ponderado em função do desempenho mensal alcançado nele. Na medição, será apurado o afastamento dos indicadores de nível de serviço em relação às metas estabelecidas em contrato, aplicando-se um Fator de Desconto (FD);

5.24.2. Nos casos em que o afastamento ensejar o desempenho abaixo da meta exigida, o valor do afastamento será utilizado para abater valores financeiros dos preços previstos em contrato;

5.24.3. Os Fatores de Desconto (FD) serão calculados com base nos resultados alcançados nos indicadores de nível de serviço, previstos nesta especificação técnica (item 5.24.9);

5.24.3.1. Haverá uma tolerância de 5% (cinco por cento) em relação à meta para a aplicabilidade do fator de desconto, ou seja, caso o índice mensurado ultrapasse a tolerância, o FD será calculado conforme o item 5.24.6.

5.24.4. No cálculo do FD está previsto uma ponderação para cada indicador de nível de serviço, denominada de Fator de Impacto no Serviço (FIS), com o objetivo de adequar os descontos ao grau de importância daquele indicador no contexto do serviço;

5.24.4.1. O FD de cada indicador será limitado à porcentagem representada pelo FIS aplicada ao valor mensal da prestação do serviço.

5.24.5. O FIS será utilizado nas situações em que a meta exigida para o indicador não for efetivamente atingida. Nos casos em que a meta exigida for atingida não haverá abatimento;

5.24.6. No valor mensal do serviço será abatido o FD calculado para cada resultado de indicador não alcançado:

$$FD_{indicador} = Valor\ Mensal \times \frac{FIS_{indicador}}{100} \times \frac{\left|Meta_{indicador} - Resultado_{indicador}\right|}{Meta_{indicador}}$$

$$FD_{total} = \sum_{i=1}^{max(indicadores)} FD_i$$

5.24.7. Além da aplicação do FD, haverá glosa adicional de 0,2% (dois décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 20% (vinte por cento) em relação à meta prevista, até o limite de 50% (cinquenta por cento). Ultrapassado esse limite, além da glosa adicional, haverá cobrança de multa, prevista no instrumento contratual;

5.24.8. Além da aplicação do FD, haverá glosa adicional de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 10% em relação à meta prevista em 3 medições consecutivas e poderá ensejar a inexecução parcial ou total do contrato;

5.24.9. Os seguintes Indicadores de Nível de Serviço serão considerados:

Item	Indicador de Nível de Serviço	Fórmula de Cálculo	Unidade de Medida	Meta exigida	Fator de Impacto no Serviço (FIS)
1	Tempo médio de triagem de requisições/incidentes	Somatório dos tempos de triagem de requisições e incidentes / Total de requisições e incidentes	minutos	<= 30	10
2	Tempo médio de resolução de requisições/incidentes de severidade crítica	Somatório dos tempos de resolução de requisições e incidentes de severidade crítica / Total de requisições e incidentes	horas	<= 1	20
3	Tempo médio de resolução de requisições/incidentes de severidade alta	Somatório dos tempos de resolução de requisições e incidentes de severidade alta / Total de requisições e incidentes	horas	<=2	20
4	Tempo médio de resolução de requisições/incidentes de severidade média	Somatório dos tempos de resolução de requisições e incidentes de severidade média / Total de requisições e incidentes	horas	<= 4	15

Item	Indicador de Nível de Serviço	Fórmula de Cálculo	Unidade de Medida	Meta exigida	Fator de Impacto no Serviço (FIS)
5	Tempo médio de resolução de requisições/incidentes de severidade baixa	Somatório dos tempos de resolução de requisições e incidentes de severidade baixa / Total de requisições e incidentes	horas	<= 12	10
6	Tempo médio de resolução de requisições de severidade agendado	Somatório dos tempos de resolução de requisições e incidentes de severidade agendado / Total de requisições e incidentes	horas	<= 24	5
7	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da CONTRATADA, na documentação dos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação dos incidentes de segurança / Tamanho da amostra x 100	%	<= 5%	10
8	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da CONTRATADA, na documentação das lições aprendidas nos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação das lições aprendidas / Tamanho da amostra x 100	%	<= 5%	5
9	Índice de qualificação da equipe conforme itens 5.29.3, 5.29.4 e 5.29.5 do Anexo I	Total de certificados da equipe / Quantidade de certificados exigidos, contabilizados depois de 90 dias do profissional entrar em operação	%	= 100%	5
10	Índice de disponibilidade da infraestrutura necessária à prestação dos serviços	A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês	%	>= 99,9%	–

5.24.10. Glosa adicional de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, por dia de atraso, caso a CONTRATADA apresente os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas (item 5.29 e subitens), em prazo superior a 5 (cinco) dias úteis até o limite de 20 (vinte) dias úteis, quando haverá, além da glosa, cobrança de multa, prevista no instrumento contratual.

5.24.11. Glosa adicional de 5% (cinco por cento) sobre o valor mensal do contrato caso a

disponibilidade de toda infraestrutura necessária à prestação dos serviços seja inferior a 99,90% (noventa e nove vírgula nove por cento) até o limite de 99% (noventa e nove por cento), quando haverá, além da glosa, cobrança de multa, prevista no instrumento contratual. A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês.

5.25. Não há previsão de bônus ou pagamentos adicionais para os casos em que a CONTRATADA superar as metas previstas, ou caso seja necessária a alocação de maior número de profissionais para o alcance das metas;

5.26. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período, nem o não atendimento da mesma meta em outro período;

5.27. Todos os indicadores que dependem de amostra para cálculo serão mensurados com método aleatório de escolha do espaço amostral definido pelo CONTRATANTE e serão aferidos com nível de confiança de 90% e margem de erro de 5%.

5.28. O CONTRATANTE comunicará a CONTRATADA sobre o recebimento definitivo a fim de possibilitar a emissão da nota fiscal, informando os valores correspondentes às glosas.

QUALIFICAÇÃO TÉCNICA

5.29. Qualificação Técnica do Quadro Profissional:

5.29.1. A CONTRATADA deve apresentar, antes da assinatura do contrato (conforme descrito no item 14 do edital), as certificações e documentos listados nos itens 5.29.3, 5.29.4 e 5.29.5 a fim de comprovar a qualificação técnica dos profissionais alocados para a prestação dos serviços.

5.29.1.1. A comprovação dos perfis exigidos para os profissionais se dará por meio de documentação das certificações (dentro do período de validade).

5.29.2. É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço (item 5.24.9) e metas estabelecidas.

5.29.3. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (Grupo 1(G1) - itens 1 a 6 da contratação).

5.29.3.1. O líder técnico (Item 5.11) deve, obrigatoriamente, ter a certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e

resposta a ataques cibernéticos.

5.29.4. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela detecção, notificação e investigação de ataques cibernéticos, deverão ter certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

5.29.4.1. CompTIA PenTest+;

5.29.4.2. EC-Concil Licensed Penetration Tester (LPT);

5.29.4.3. IACRB Certified Expert Penetration Tester (CEPT);

5.29.4.4. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

5.29.4.5. GIAC Reverse Engineering Malware (GREM);

5.29.4.6. Offensive Security Certified Professional (OSCP);

5.29.4.7. Ethical Hacking Post Exploitation (EHPX);

5.29.4.8. Offensive Security Experienced Penetration Tester (OSEP);

5.29.4.9. Offensive Security Web Expert (OSWE);

5.29.4.10. Certified Red Team Expert (CRTE);

5.29.4.11. Offensive Security Certified Expert (OSCE);

5.29.4.12. Certified Ethical Hacker (CEH).

5.29.5. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

5.29.5.1. Certified Information Security Manager (CISM);

5.29.5.2. GIAC Experienced Cybersecurity Specialist (GX-CS);

5.29.5.3. GIAC Reverse Engineering Malware (GREM);

5.29.5.4. Ethical Hacking Post Exploitation (EHPX);

5.29.5.5. CompTIA Security+;

5.29.5.6. CompTIA Advanced Security Practitioner;

5.29.5.7. EC-Council Security Analyst (ECSA);

5.29.5.8. Certified Information Systems Security Professional (CISSP);

5.29.5.9. CompTIA CYSA+ - Cybersecurity Analyst.

5.29.6. Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a CONTRATADA, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

5.29.7. A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

5.29.8. O CONTRATANTE se reserva ao direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

ANEXO VIII

TERMO DE CONFIDENCIALIDADE - CONTRATADA

CONTRATO Nº 097/2024

A contratada **CONSÓRCIO PETASERVICE SEC**, doravante referida simplesmente como CONTRATADA, inscrita no CNPJ/MF sob o número **57.413.479/0001-05**, com endereço em SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília-DF - CEP 70.200-002, neste ato representada pelo sócio-diretor José André Mendes Coimbra, nos termos do Contrato nº 097/2024, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante o **TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO**, doravante referido simplesmente como CONTRATANTE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº 097/2024.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação revelada à CONTRATADA.

Subcláusula Segunda - A CONTRATADA reconhece que, em razão da prestação de serviços ao CONTRATANTE, tem acesso a informações que pertencem ao CONTRATANTE, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, em decorrência da execução do contrato, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, projetos, outras informações técnicas, jurídicas, financeiras ou

comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do CONTRATANTE, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do CONTRATANTE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que seja comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

A CONTRATADA se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente para os propósitos do contrato.

Subcláusula Primeira - A CONTRATADA determinará a observância deste TERMO DE CONFIDENCIALIDADE, bem como a observância e a assinatura do TERMO DE CONFIDENCIALIDADE - COLABORADOR, a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato.

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Subcláusula Terceira - Compromete-se, ainda, a CONTRATADA a não revelar, reproduzir ou utilizar, bem como não permitir que seus empregados, prepostos ou prestadores de serviço revelem, reproduzam ou utilizem, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas no contrato e neste TERMO DE CONFIDENCIALIDADE.

Subcláusula Quarta - A CONTRATADA deve cuidar para que as informações consideradas confidenciais nos termos do presente TERMO DE CONFIDENCIALIDADE fiquem restritas ao conhecimento dos empregados, prepostos ou prestadores de serviço que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios, devendo cientificá-los da existência deste TERMO DE CONFIDENCIALIDADE e da natureza confidencial das informações.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente ao CONTRATANTE, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com o CONTRATANTE.

CLÁUSULA SEXTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

CLÁUSULA SÉTIMA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente TERMO DE CONFIDENCIALIDADE, após o término do Contrato.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo CONTRATANTE.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, data da última assinatura eletrônica.

Assinado digitalmente
VALDIR FLORINDO
Desembargador Presidente do Tribunal

Assinado digitalmente
JOSÉ ANDRÉ MENDES COIMBRA
Consórcio Petaservice Sec.

TESTEMUNHAS:

Assinado digitalmente
CLAUDIA SANT'ANNA PINHEIRO
Diretora da Coordenadoria de Segurança de TIC

Assinado digitalmente
MARCIO NISI GONÇALVES
Diretor da Secretaria de Tecnologia da Informação e Comunicações

ANEXO IX

TERMO DE CONFIDENCIALIDADE - COLABORADOR DA CONTRATADA

A **<PESSOA FÍSICA OU JURÍDICA>**, doravante referida simplesmente como COLABORADOR, inscrita no CPF/CNPJ sob o número **<NÚMERO DO CPF/CNPJ>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas aos empregados, prepostos ou prestadores de serviço de empresas contratadas pelo <TRIBUNAL> (<SIGLA DO TRIBUNAL>), para que possam desenvolver suas atividades institucionais.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação.

Subcláusula Segunda – O COLABORADOR reconhece que tem acesso a informações que pertencem ao <SIGLA DO TRIBUNAL>, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, projetos, outras informações técnicas, jurídicas,

financeiras ou comerciais, entre outras a que venha o COLABORADOR ter acesso durante ou em razão da execução de suas atividades profissionais.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, o COLABORADOR deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do <SIGLA DO TRIBUNAL>, a tratá-la diferentemente. Em hipótese

alguma, a ausência de manifestação expressa do <SIGLA DO TRIBUNAL>poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que:

I - sejam comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão do COLABORADOR;

II - já esteja em poder do COLABORADOR, como resultado de sua própria pesquisa, contanto que o COLABORADOR possa comprovar referido fato; ou

III - tenha sido comprovada e legitimamente recebida de terceiros, contanto que o COLABORADOR possa comprovar referido fato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

O COLABORADOR se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente no desempenho de suas atividades profissionais enquanto contratado.

Subcláusula Primeira - Compromete-se, ainda, o COLABORADOR a não revelar, reproduzir ou utilizar, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas neste documento.

CLÁUSULA QUINTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

CLÁUSULA SEXTA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanecem em vigor os deveres de sigilo e de não utilização das informações, tratados no presente TERMO DE CONFIDENCIALIDADE, após o término do vínculo contratual.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo <SIGLA DO TRIBUNAL>.

Por estar de acordo, o COLABORADOR firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

_____

Nome:

Cargo / Função:

Empresa: