

CONTRATO Nº 2022/0281-01-00 PARA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, CONFORME ESPECIFICAÇÕES TÉCNICAS, QUE ENTRE SI CELEBRAM, A "SÃO PAULO TRANSPORTE S/A" E A EMPRESA "KRYPTUS SEGURANÇA DA INFORMAÇÃO S/A", NA FORMA ABAIXO MENCIONADA:

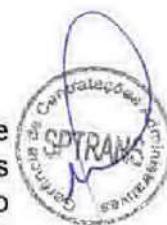


Pelo presente instrumento e na melhor forma de direito, a **SÃO PAULO TRANSPORTE S/A**, sociedade de economia mista, com sede nesta Capital, na Rua Boa Vista, nº 236, cadastrada no CNPJ/MF sob nº 60.498.417/0001-58, neste ato representada por seu Diretor e por seu Procurador ao final nomeados e qualificados, que este subscrevem, em conformidade com seu Estatuto Social, doravante denominada simplesmente "**SPTTrans**", e de outro a empresa **KRYPTUS SEGURANÇA DA INFORMAÇÃO S/A**, com sede na Cidade de Campinas - SP, na Rua Maria Tereza Dias da Silva, nº 270, Bairro Cidade Universitária, inscrita no CNPJ/MF sob nº 05.761.098/0001-13, neste ato representada por seus Diretores, ao final nomeados e qualificados, que também subscrevem o presente, doravante denominada simplesmente **CONTRATADA**, consoante autorização desta contratação no Termo de Homologação publicado no Diário Oficial da Cidade em 16/09/2022, vinculado aos termos do Edital da **LICITAÇÃO**, pelo rito da modalidade de **PREGÃO** na forma **ELETRÔNICA**, sob nº **010/2022**, do tipo menor preço, cuja contratação se dará sob o regime de empreitada por preços unitários, Processo Administrativo de Licitações e Contratos - **PALC** nº **2022/0281**, com a finalidade de manutenção da segurança da informação, e será regido pela Lei Federal nº 13.303, de 30/06/16, Lei Complementar nº 123, de 14/12/06 e alterações; Decreto Municipal nº 56.475, de 05/10/15; Lei Municipal nº 14.094, de 06/12/05 e Regulamento Interno de Licitações e Contratos da **SPTTrans** - **RILC**, disponível no link http://www.sptrans.com.br/media/1158/regulamento_interno_licitacoes_e_contratos_out18.pdf, que foi publicado no Diário Oficial da Cidade em 18/10/18, Código de Conduta e Integridade da **SPTTrans**, disponível no link <http://dados.prefeitura.sp.gov.br/dataset/0555564c-5e1d-4179-a6eb-fa7ef8223474/resource/54514465-e36f-41b3-b129-95dc2cd6794a/download/codconduta2.pdf>, preceitos de direito privado, bem como demais diplomas aplicáveis à espécie, têm entre si justo e avençado o seguinte:

(SEI 5010.2022/0016218-4)

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente contrato tem por objeto a prestação de serviços gerenciados de segurança da informação, compreendendo o monitoramento de comportamentos que apresentem risco e vulnerabilidades em regime 24x7, suportar a SPTRANS no direcionamento do tratamento de incidentes de segurança, treinamento da equipe e suporte a implantação de boas práticas, conforme especificações técnicas.



CLÁUSULA SEGUNDA - DOS DOCUMENTOS INTEGRANTES

- 2.1. Integram o presente contrato tal como se nele estivessem transcritos os documentos a seguir relacionados:
- 2.1.1. Anexo II – Termo de Referência;
 - 2.1.2. Anexo III – Planilha de Quantidades e Preços, da **CONTRATADA**;
 - 2.1.3. Anexo IV – Composição da Taxa de BDI, da **CONTRATADA**;
 - 2.1.4. Anexo V – Composição da Taxa de Encargos Sociais, da **CONTRATADA**;
 - 2.1.5. Anexo VI – Critério de Preço e Medição;
 - 2.1.6. Anexo VIII – Carta Proposta Comercial, e Prorrogação da Proposta, respectivamente de 16/08/2022, e de 13/10/2022, da **CONTRATADA**;
 - 2.1.7. Composições de Preços Unitários, da **CONTRATADA**.

CLÁUSULA TERCEIRA - DOS PRAZOS

- 3.1. O prazo de vigência do contrato será de **60 (sessenta) meses**, contados a partir da data de assinatura do contrato.

CLÁUSULA QUARTA - DOS RECURSOS ORÇAMENTÁRIOS E FINANCEIROS

- 4.1. Os recursos necessários para suportar as despesas deste instrumento, no presente exercício, constam da "Previsão Orçamentária de 2022 da SPTTrans", conforme Requisição de Compra – RC nº 27510.
- 4.1.1. Para os exercícios seguintes, ficam condicionados à aprovação das respectivas Leis Orçamentárias.

CLÁUSULA QUINTA - DO VALOR

- 5.1. Tem o presente contrato o valor total de R\$ 23.600.000,00 (vinte e três milhões e seiscentos mil reais), referido ao mês da data da apresentação da proposta, ou seja, agosto/2022.

CLÁUSULA SEXTA – DA PRESTAÇÃO DO SERVIÇO

- 6.1. A **CONTRATADA** deverá obedecer as condições estabelecidas no Anexo II - Termo de Referência.
- 6.2. Para início pleno dos serviços, a **CONTRATADA** deverá estar com todas as funcionalidades descritas no Anexo II - Termo de Referência em operação em até 10 (dez) dias corridos, a contar da data de assinatura do contrato.



- 6.3. Deverá a **CONTRATADA** prover todo serviço de segurança para a infraestrutura de TI da SPTRANS em regime 24/7, conforme descrito no item 2 do Anexo II – Termo de Referência.
- 6.4. A **CONTRATADA** deverá prover um Portal Web, telefone e/ou e-mail, para abertura dos chamados técnicos.
- 6.5. A **CONTRATADA** deverá efetuar toda prestação de serviço para todo ambiente computacional da **SPTRANS**, ou seja, todos os sistemas interligados (Corporativo, Monitoramento, Sistema de Bilhetagem Eletrônica, etc), bem como toda a infraestrutura que o comportam;
- 6.6. A **CONTRATADA** deverá prover treinamento conforme estabelecido no Anexo II - Termo de Referência.

CLÁUSULA SÉTIMA – DOS PREÇOS E REAJUSTAMENTO

- 7.1. Para todos os serviços, objeto deste contrato, serão adotados os preços unitários propostos pela **CONTRATADA** constantes no Anexo III – Planilha de Quantidades e Preços, referidos ao mês da data de apresentação das propostas, ou seja, agosto/2022.
- 7.2. Nos preços unitários propostos que constituirão a única e completa remuneração para a execução do objeto do contrato, estão computados todos os custos, tributos e despesas da **CONTRATADA**, conforme o contido no Anexo VI - Critério de Preço e Medição, nada mais podendo a **CONTRATADA** pleitear a título de pagamento, reembolso ou remuneração em razão do contrato, de sua celebração e cumprimento.
 - 7.2.1. Quaisquer tributos ou encargos legais, criados, alterados ou extintos, após a assinatura do contrato, de comprovada repercussão nos preços contratados, implicarão a revisão destes para mais ou para menos, conforme o caso.
 - 7.2.2. Caso a **SPTrans** ou a **CONTRATADA** venha a obter das autoridades governamentais benefícios fiscais, isenções ou privilégios referentes a tributos incidentes sobre os preços do objeto deste contrato, as vantagens decorrentes desses incentivos determinarão a redução de preço, na medida em que sobre eles repercutirem.
- 7.3. Os preços contratuais propostos serão reajustados obedecido o seguinte critério:

- 7.3.1. Na conformidade com a legislação vigente, o reajuste dos preços contratados será calculado de acordo com a seguinte fórmula:

$$R = P_0 \times \left[\left(\frac{\text{IPC FIPE}_1}{\text{IPC FIPE}_0} \right) - 1 \right]$$

ONDE:

R = Valor do reajustamento.



X

OY

P_0 = Valor da medição calculada com os preços do contrato, base agosto/2022.

IPC-FIPE₀ = Número Índice de Preços ao Consumidor – IPC apurado pela Fundação Instituto de Pesquisas Econômicas - FIPE, referente ao mês da base dos preços, isto é, agosto/2022.

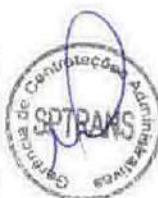
IPC-FIPE₁ = Número Índice de Preços ao Consumidor – IPC apurado pela Fundação Instituto de Pesquisas Econômicas - FIPE, referente ao mês de anualização da base de preços, isto é, agosto/2023, e agosto dos anos subsequentes, no caso de prorrogação do prazo contratual.

- 7.3.2. O reajustamento obedecerá às disposições contidas na Portaria SF nº 389 de 18 de dezembro de 2017 ou em outro dispositivo legal que venha a substituí-la.
- 7.3.3. O cálculo do reajuste se dará em função da variação ocorrida entre o mês da data base agosto/2022 e o mês de sua anualização, agosto/2023, e vigorará sobre os preços contratuais a partir do mês de agosto/2023 e agosto dos anos subsequentes, no caso de prorrogações de prazo contratual.
- 7.3.4. O percentual de reajuste será calculado considerando 2 (duas) casas decimais, efetuando-se o arredondamento por critério matemático. Exemplo: 5,425% será arredondado para 5,43%; 5,424% será arredondado para 5,42%.
- 7.3.5. O valor referente ao reajuste de preços somente será exigível no primeiro pagamento devido à **CONTRATADA**, depois de transcorridos 12 (doze) meses da data estabelecida como "data base" do preço (P_0) e após a divulgação oficial do índice adotado na fórmula acima, sendo vedada a aplicação do índice provisório.
- 7.3.6. A aplicação de novos reajustes deverá considerar a data e os valores do reajuste anterior, restando vedada a aplicação de índices acumulados por um período superior a 12 (doze) meses.

CLÁUSULA OITAVA – DA MEDIÇÃO, ACEITAÇÃO E FORMA DE PAGAMENTO

- 8.1. As medições dos serviços serão apresentadas mensalmente pela **CONTRATADA**, mediante relatório detalhado dos serviços executados no período para apuração de SLA, conforme o Anexo II - Termo de Referência e Anexo VI - Critério de Preço e Medição, cabendo à área gestora a aferição dos quantitativos e qualidade do serviço prestado.

- 8.1.1. A primeira será realizada no 26º (vigésimo sexto) dia do mês, considerando-se como primeiro dia da contagem, a data do efetivo início dos serviços.
- 8.1.2. As subsequentes suceder-se-ão a cada período de 1 (um) mês, a partir do término da medição anterior, exceto a medição final, que poderá abranger menor período, por se tratar do último da execução do objeto.



X

Y

- 8.1.3. Para efeito do cálculo *pro-rata* considerar-se-á mês comercial de 30 (trinta) dias.
- 8.1.4. A **SPTTrans** somente autorizará a emissão das notas fiscais/faturas, após a emissão do Termo de Aceitação da Medição pela **SPTTrans**.
- 8.1.4.1. A **CONTRATADA** deverá emitir nota fiscal em separado, de acordo com o valor e respectiva fonte de recurso, informado pela **SPTTrans**, na aceitação formal da medição.
- 8.1.5. No 1º (primeiro) dia útil do mês subsequente, a **CONTRATADA** emitirá as Notas Fiscais/Faturas referentes aos serviços prestados no mês anterior.
- 8.2. Os pagamentos serão efetuados 30 (trinta) dias após a data de apresentação e aceite pela **SPTTrans** da(s) nota(s) fiscal(is), devidamente atestada pela área gerenciadora dos serviços, por meio de crédito em conta corrente que a **CONTRATADA** deverá manter no banco a ser indicado pela **SPTTrans**.
- 8.3. A **CONTRATADA** deverá entregar uma carta padrão de autorização de crédito em conta corrente na Gerência de Finanças – DA/SFI/GFI, na Rua Boa Vista, nº 236 – 2º andar, fundos – Centro – CEP 01014-020 – São Paulo – SP, conforme Anexo IX - Carta de Autorização de Crédito em Conta Corrente.
 - 8.3.1. Caso a **CONTRATADA** solicite que o pagamento seja creditado em conta corrente de outro banco que não o indicado pela **SPTTrans**, arcará com todas as despesas e tarifas bancárias vigentes, incorridas na transação de pagamento: DOC, TED, Tarifa de emissão de cheque e outras.
 - 8.3.2. Admitido o pagamento com o código de barras, no entanto, caso ocorra algum imprevisto junto à instituição bancária, o pagamento poderá ser efetuado conforme descrito no item 8.2 com posterior envio do comprovante de depósito por e-mail cadastrado em nosso controle interno fornecido pela empresa.
- 8.4. No caso de eventual atraso no pagamento pela **SPTTrans**, o valor devido será atualizado financeiramente, *pró-rata temporis*, mediante manifestação expressa da **CONTRATADA**, desde o dia de seu vencimento até a data de seu efetivo pagamento, nas condições estabelecidas pela Portaria nº 05/12 expedida pela Secretaria Municipal da Fazenda da Prefeitura de São Paulo e, na ausência destas, pelo IPCA (IBGE). Para efeito deste cálculo, considerar-se-á mês comercial de 30 (trinta) dias.
 - 8.4.1. Essa atualização não será aplicada na hipótese de suspensão do pagamento, em razão do cumprimento da Lei Municipal nº 14.094/2005, ou seja, caso a **CONTRATADA** esteja inscrita no CADIN Municipal.
- 8.5. As notas fiscais deverão ser entregues na Rua Boa Vista, 236, 6º andar – Centro – São Paulo – SP, aos cuidados do Sr. Maurício Lima Ferreira - DG/STI, no horário compreendido entre 09h00 e 17h00, de segunda a sexta-feira.



- 8.6. Realizada a medição, a **CONTRATADA** enviará o respectivo relatório de medição dos serviços à **SPTTrans** até o 1º (primeiro) dia útil subsequente ao término da prestação de serviço, sendo que a **SPTTrans** terá o prazo de 2 (dois) dias úteis do recebimento, para aceitá-la.
- 8.7. A efetivação do pagamento à **CONTRATADA** fica condicionada à ausência de registro no CADIN – Municipal, nos termos da Lei Municipal nº 14.094/05.
- 8.8. As notas fiscais (documentos de cobrança) emitidas pela **CONTRATADA** deverão mencionar os seguintes dados:
- 8.8.1. Endereço: Rua Boa Vista, 236 - Centro - CEP 01014-000 - São Paulo/SP;
- 8.8.2. CNPJ 60.498.417/0001-58 Inscrição e Estadual (isenta);
- 8.8.3. Número de registro do contrato e item contratual;
- 8.8.4. Objeto contratual;
- 8.8.5. Mês a que se refere a prestação de serviços;
- 8.8.6. Valor correspondente à retenção do Imposto de Renda Retido na Fonte (IRRF) e das Contribuições Sociais (PIS-PASEP/COFINS/CSLL).
- 8.9. No caso da **CONTRATADA** não ser obrigada a destacar a retenção na fonte, dos impostos e contribuições acima relacionados, deverá discriminá-la nas notas fiscais/faturas os devidos enquadramentos legais e anexar os documentos comprobatórios.
- 8.10. Se a **CONTRATADA** for optante do Simples Nacional, também deverá apresentar a devida comprovação, a cada faturamento, a fim de evitar a retenção, na fonte, dos tributos e contribuições, conforme legislação em vigor.
- 8.11. A **CONTRATADA** dará como quitadas as duplicatas e outros documentos de cobrança emitidos contra a **SPTTrans**, pela efetivação do crédito em conta corrente.
- 8.11.1. Quaisquer outros títulos emitidos pela **CONTRATADA** deverão ser mantidos em carteira, não sendo a **SPTTrans** obrigada a efetuar o seu pagamento, se colocados em cobrança pelo sistema bancário.
- 8.11.2. Quaisquer pagamentos não isentará a **CONTRATADA** das responsabilidades contratuais, nem implicarão na aceitação definitiva dos serviços.
- 8.12. A **SPTTrans** poderá descontar de qualquer pagamento, importância que a qualquer título lhe seja devida pela **CONTRATADA**, por força deste ou de outros contratos, garantidos os princípios do contraditório e ampla defesa quando for o caso.
- 8.13. A **SPTTrans** poderá sustar o pagamento de qualquer fatura, na hipótese da inobservância, pela **CONTRATADA**, de suas obrigações tributárias, até a comprovação da regularidade.

CLÁUSULA NONA – DAS GLOSAS

- 9.1. A glosa do mês de competência dos serviços será aplicada no próprio mês da sua prestação.



- 9.2. A SPTTrans informará à **CONTRATADA**, quanto à existência de glosa, no dia útil imediatamente posterior e autorizará a emissão de nota fiscal/fatura já deduzido o valor da glosa.

- 9.3. O questionamento de glosa por parte da **CONTRATADA** poderá ser apresentado até o próximo dia útil ao da comunicação da glosa pela **SPTTrans**.

Fórmula e parâmetros para o cálculo da glosa:

$$G = (VCL/HM) * TIND$$

onde:

G = Glosa;

VCL = Valor da Parcela Mensal do Contrato;

HM = Hora mês;

TIND = Tempo de Indisponibilidade.

Exemplo de 4 horas (incluindo o tempo do SLA): (R\$20.000,00/720) * 4
R\$ 27,78*4 = R\$ 111,12

CLÁUSULA DÉCIMA - DAS RESPONSABILIDADES E OBRIGAÇÕES

- 10.1. São obrigações da **CONTRATADA**, além das demais previstas no contrato:

- 10.1.1. Ter pleno conhecimento das condições contratuais, pelo que reconhece ser perfeitamente viável o cumprimento integral e pontual dos encargos assumidos.
- 10.1.2. Ser responsável pelos danos causados à **SPTTrans** ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato.
- 10.1.3. Não prestar informações de qualquer ordem a terceiros, técnicas ou não, sobre a natureza ou execução do presente contrato, ou divulgá-las por qualquer forma, sem prévia autorização expressa da **SPTTrans**.
- 10.1.4. Informar à **SPTTrans**, a qualquer tempo, a ocorrência das seguintes situações:
- 10.1.4.1. Declaração de inidoneidade por ato do Poder Público;
- 10.1.4.2. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração;
- 10.1.4.3. Impedimento de licitar, de acordo com o previsto na legislação vigente.

- 10.2. Se a **CONTRATADA** desejar, para fins promocionais ou publicitários, divulgar o serviço a seu cargo, somente poderá fazê-lo mediante apresentação prévia do material de divulgação e sua aprovação expressa pela **SPTTrans**.



Y

JY

- 10.3. Na execução do presente contrato, a **CONTRATADA** estará obrigada, em especial, a prestar os serviços objeto do contrato, estritamente de acordo com as especificações técnicas dentro dos prazos estabelecidos e obrigações nos termos do Anexo II – Termo de Referência.
 - 10.4. A **CONTRATADA** deve manter, durante a execução do contrato, todas as condições de habilitação exigidas na licitação que deu origem ao presente instrumento (artigo 109, inciso XV do RILC).
 - 10.5. A fiscalização e/ou o acompanhamento exercidos por representantes da **SPTTrans** não excluirá ou reduzirá as responsabilidades assumidas pela **CONTRATADA**.
 - 10.6. As providências e despesas relativas ao pagamento de qualquer tributo que incida ou venha a incidir sobre o contrato serão de exclusiva responsabilidade da **CONTRATADA**.
 - 10.7. Ainda que a prestação dos serviços esteja concluída e que todos os relatórios e demais documentos relativos a este contrato já tenham sido entregues à **SPTTrans**, e mesmo que esteja encerrado o prazo contratual, a **CONTRATADA** ficará responsável por quaisquer esclarecimentos que se fizerem necessários, a critério da **SPTTrans**, bem como por eventuais vícios posteriormente detectados nos serviços prestados.
- 10.8. São obrigações da **SPTTrans**:**
- 10.8.1. Prestar todas as informações e tomar as decisões em tempo hábil, necessárias à execução do objeto do contrato e ao desenvolvimento dos trabalhos pela **CONTRATADA**.
 - 10.8.2. Auxiliar a **CONTRATADA**, quando necessário, na interface e tramitação de documentos.
 - 10.8.3. Acompanhar e fiscalizar a execução do contrato por meio de representante designado para esse fim, objetivando verificar a aderência pela **CONTRATADA** aos termos do presente contrato.
 - 10.8.4. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

- 10.9. A **SPTTrans** e a **CONTRATADA**, pelo presente instrumento, concordam que constitui responsabilidade de ambas as Partes a observância das normas da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e daquelas constantes de ulteriores regulamentos que venham a dispor sobre a proteção de dados pessoais, inclusive os que vierem a ser editados pela Autoridade Nacional de Proteção de Dados – ANPD.**

- 10.9.1. Quando da realização das atividades de tratamento de dados pessoais, inclusive daqueles considerados sensíveis, a **CONTRATADA** executará o objeto deste Contrato de forma a observar, em especial, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos



22

dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

- 10.9.2. Durante a vigência deste Contrato, a SPTTrans poderá recusar a adoção de procedimentos internos da CONTRATADA relacionados à execução do objeto pactuado que eventualmente contrariem ou que visem a frustrar os direitos, deveres, fundamentos, princípios ou os objetivos constantes dos instrumentos legais e regulamentares sobre proteção de dados pessoais, podendo a SPTTrans emitir instruções lícitas à CONTRATADA com vistas a garantir o exato cumprimento da LGPD.
- 10.9.3. A SPTTrans e a CONTRATADA concordam, no âmbito da política de governança de cada uma e visando coibir a ocorrência de danos em virtude do tratamento de dados pessoais, em adotar medidas técnicas e administrativas preventivas e eficazes que sejam aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
 - 10.9.3.1. As Partes poderão alterar ou substituir as medidas mencionadas no subitem 10.9.3. por outras a qualquer momento e sem notificação prévia, desde que as novas atendam ao mesmo propósito das anteriores e desde que mantenham um nível de segurança, em proteção dos dados pessoais tratados, equivalente ou superior.
- 10.9.4. As Partes comprometem-se a cooperar entre si para lidarem, em tempo razoável e no âmbito da execução do objeto deste Contrato, com as eventuais solicitações feitas pelos titulares ou pelas autoridades regulatórias em relação aos dados pessoais tratados e em relação a algum eventual caso de violação.

CLÁUSULA DÉCIMA PRIMEIRA - DA GARANTIA CONTRATUAL

- 11.1. A CONTRATADA deverá apresentar à SPTTrans garantia de execução contratual, no prazo de até 10 (dez) dias úteis após a celebração do respectivo instrumento, sob pena de aplicação das sanções cabíveis, especialmente a multa prevista no subitem 12.2.1 deste contrato, devendo a vigência da garantia ter seu início na mesma data de assinatura do contrato.
- 11.2. A garantia será de R\$ 1.180.000,00 (um milhão, cento e oitenta mil reais), equivalente a 5% (cinco por cento) do valor do contrato e será atualizada, nas mesmas condições, na hipótese de modificação do contrato originalmente pactuado.
- 11.3. Caberá à CONTRATADA optar por uma das seguintes modalidades de garantia:
 - 11.3.1. Caução em dinheiro;
 - 11.3.2. Seguro-garantia;
 - 11.3.3. Fiança bancária.



- 11.4. Se a **CONTRATADA** optar pela apresentação de garantia na modalidade Seguro-garantia o ramo deverá ser o seguinte: Seguro Garantia: Segurado – Setor Público, conforme artigos 3º e 4º da Circular Susep nº 477 de 30 de setembro de 2013.
- 11.5. A garantia prestada por meio de seguro-garantia ou carta fiança deverá ter prazo de vigência superior em 180 (cento e oitenta) dias à vigência do contrato.
- 11.5.1. A garantia prestada na modalidade de fiança bancária ou seguro garantia deverá ser apresentada na forma digital ou em original com reconhecimento de firma e apresentação de procuração atualizada. As garantias efetuadas de forma digital, somente serão reconhecidas após a sua verificação junto ao site da SUSEP (Superintendência de Seguros Privados).
- 11.5.2. A admissibilidade de Apólice de Seguro com Selo de Autenticidade, passível de verificação na SUSEP, nos termos da MP nº 2.200-2/2001 de 24/08/2001, não isenta a **CONTRATADA** da responsabilidade pela autenticidade do documento apresentado.
- 11.5.3. Constatada qualquer irregularidade na conferência da autenticidade, deverá ser providenciada a imediata substituição da garantia.
- 11.6. O atraso superior a 25 (vinte e cinco) dias para a apresentação da garantia a que se refere o item 11.1. autorizará a **SPTTrans** a buscar a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, sem prejuízo da aplicação de outras sanções previstas no RILC e neste Contrato.
- 11.7. A garantia deverá ser complementada pela **CONTRATADA** sempre que, independente do motivo, houver elevação no valor contratual.
- 11.8. A garantia será liberada para devolução após cumprimento definitivo do contrato, mediante solicitação por escrito da **CONTRATADA** ao gestor do contrato, desde que não haja multas a aplicar, acerto de contas por fazer, pendências trabalhistas, previdenciárias, fundiárias (FGTS) ou de qualquer outra natureza, e ainda, após a assinatura, pelas partes, do "Termo de Conclusão, Encerramento e Quitação".
- 11.9. Para a devolução da garantia prestada em moeda corrente nacional o valor devido será atualizado financeiramente *pró-rata temporis* - desde a data do recolhimento até a data da efetiva devolução da garantia ou no caso de substituição da garantia, até a data da comunicação à **SPTTrans** para sua liberação - nas condições estabelecidas para a matéria em regulamentações expedidas pela Secretaria Municipal da Fazenda da Prefeitura de São Paulo e na ausência destas pelo IPCA (IBGE). Para efeito deste cálculo considerar-se-á como data final a correspondente aos últimos números-índices publicados, estabelecendo-se o mês comercial de 30 (trinta) dias.
- 11.10. A garantia de execução contratual poderá ser alterada quando conveniente a sua substituição a pedido da **CONTRATADA** e desde que aceita pela **SPTTrans**, observado o disposto no item 11.9.



2/2

11.11. A garantia contratual responderá pelas multas aplicadas, por indenizações devidas e por quaisquer pendências contratuais existentes.

CLÁUSULA DÉCIMA SEGUNDA - DAS ALTERAÇÕES, RESCISÃO, RECURSO, PENALIDADES

12.1. Este contrato, regido pelo RILC, poderá ser alterado qualitativa e quantitativamente, por acordo das partes e mediante prévia justificativa da autoridade competente, vedando-se alterações que resultem em violação ao dever de licitar.

12.1.1. A alteração qualitativa do objeto poderá ocorrer quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos objetivos da SPTTrans.

12.1.2. A alteração quantitativa poderá ocorrer, nas mesmas condições contratuais, quando forem necessários acréscimos ou supressões do objeto até o limite máximo de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

12.1.3. Nenhum acréscimo ou supressão poderá exceder o limite estabelecido no subitem 12.1.2, salvo as supressões resultantes de acordos celebrados entre os contratantes.

12.2. As Sanções obedecerão aos artigos 240 e seguintes do RILC e, ainda, às seguintes penalidades:

12.2.1. Multa de 1% (um por cento) sobre o valor da garantia, pelo atraso na entrega da garantia.

12.2.2. Multa de 20% (vinte por cento) sobre o valor total do contrato, em caso de **inexecução total**. Entende-se como inexecução total do contrato:

12.2.2.1. A não operação de todas as funcionalidades descritas no Termo de Referência em até 20 (vinte) dias corridos contados da data prevista para o início da operação.

12.2.3. Multa de 15% (quinze por cento) sobre o valor da parcela não executada, em caso de **inexecução parcial**: Entende-se como inexecução parcial:

12.2.3.1. A não operação de todas as funcionalidades descritas no Termo de Referência, a partir do 1º até o 19º da data prevista para o inicio da operação;

12.2.3.2. A suspensão, paralisação, ou interrupção dos serviços objeto deste contrato, sem a devida justificativa previamente aceita pela SPTTrans.

12.2.4. Multas pelo **descumprimento** do contrato, por evento:

12.2.4.1. Multa de 10% (dez por cento) sobre o valor da parcela por deixar de prestar o serviço de treinamento;



8

101

JY

- 12.2.4.2.** Multa de 2% (dois por cento) sobre o valor total atualizado do contrato pela não manutenção da certificação da equipe técnica conforme o Anexo II - Termo de Referência durante a execução contratual.
- 12.2.4.3.** Multa de 0,5% (meio por cento) sobre o valor remanescente do contrato pelo não atendimento a exigência contratual para a qual não seja cominada penalidade específica.
- 12.3.** As penalidades ora previstas serão aplicadas pela **SPTTrans** quando não forem aceitas as competentes justificativas da **CONTRATADA**, devidamente fundamentadas, instruídas em processo administrativo.
- 12.4.** Para a aplicação de penalidades serão observados os procedimentos contidos no artigo 248 e seguintes do RILC, garantido o direito ao exercício do contraditório e da ampla defesa.
- 12.5.** Constitui falta grave por parte da **CONTRATADA** o não pagamento de salário, de vale-transporte e de auxílio alimentação dos empregados na data fixada, o que poderá dar ensejo à rescisão do contrato, sem prejuízo da aplicação das sanções cabíveis.
- 12.6.** A inexecução total ou parcial do contrato poderá ensejar a sua rescisão, com as consequências cabíveis. Constituirão motivo para rescisão do contrato:
- 12.6.1. O descumprimento de obrigações contratuais;
- 12.6.2. A alteração da pessoa da contratada, mediante:
- 12.6.2.1. A subcontratação parcial do seu objeto, a cessão ou transferência, total ou parcial, a quem não atenda às condições de habilitação e sem prévia autorização da **SPTTrans**, observado o RILC;
- 12.6.3. O desatendimento das determinações regulares do gestor ou fiscal do contrato;
- 12.6.4. O cometimento reiterado de faltas na execução contratual;
- 12.6.5. A dissolução da sociedade **CONTRATADA**;
- 12.6.6. A decretação de falência da **CONTRATADA**;
- 12.6.7. A alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, desde que prejudique a execução do contrato;
- 12.6.8. Razões de interesse da **SPTTrans**, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;
- 12.6.9. O atraso nos pagamentos devidos pela **SPTTrans** decorrentes de serviços, ou parcelas destes, já executados, salvo em caso de



Y
DZ

calamidade pública, grave perturbação da ordem interna ou guerra, assegurado a **CONTRATADA** o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

- 12.6.10. A ocorrência de caso fortuito, força maior ou fato do princípio, regularmente comprovada, impeditiva da execução do contrato;
 - 12.6.11. A não integralização da garantia de execução contratual no prazo estipulado;
 - 12.6.12. O descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;
 - 12.6.13. O perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença;
 - 12.6.14. Ter sido frustrado ou fraudado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; ter sido impedida, perturbada ou fraudada a realização de qualquer ato de procedimento licitatório público; o afastamento ou a tentativa de afastamento de licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; fraude em licitação pública ou contrato dela decorrente; ter sido criada, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; a obtenção de vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ter sido manipulado ou fraudado o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; ter sido dificultada a atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização.
 - 12.6.15. O descumprimento das obrigações trabalhistas ou a perda das condições de habilitação da **CONTRATADA**.
- 12.7. Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo, devendo ser assegurado o contraditório e o direito de prévia e ampla defesa.
- 12.8. A rescisão do contrato poderá ser:
- 12.8.1. Por ato unilateral e escrito de qualquer das partes;
 - 12.8.2. Amigável, por acordo entre as partes, reduzida a termo no processo de contratação, desde que haja conveniência para a **SPTTrans**;
 - 12.8.3. Judicial, nos termos da legislação.



- 12.9. A rescisão por ato unilateral a que se refere o subitem 12.8.1 deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 30 (trinta) dias.
- 12.10. Quando a rescisão ocorrer sem que haja culpa da outra parte contratante, será esta resarcida dos prejuízos que houver sofrido, regularmente comprovados, e no caso da **CONTRATADA** terá esta ainda direito a:
- 12.10.1. Devolução da garantia;
 - 12.10.2. Pagamentos devidos pela execução do contrato até a data da rescisão.
- 12.11. A rescisão por ato unilateral da **SPTTrans** acarretará as seguintes consequências, sem prejuízo das sanções previstas neste contrato e no RILC:
- 12.11.1. Assunção imediata do objeto contratado, pela **SPTTrans**, no estado e local em que se encontrar;
 - 12.11.2. Execução da garantia contratual, para ressarcimento pelos eventuais prejuízos sofridos pela **SPTTrans**;
 - 12.11.3. Na hipótese de insuficiência da garantia contratual, a retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à **SPTTrans**;
 - 12.11.4. Caso a garantia contratual e os créditos da **CONTRATADA**, decorrentes do contrato, sejam insuficientes, ajuizamento de ação judicial com vistas à obtenção integral do ressarcimento.

CLÁUSULA DÉCIMA TERCEIRA - DA SUBCONTRATAÇÃO

- 13.1. A **CONTRATADA** poderá, mediante prévia aprovação da **SPTTrans**, subcontratar a execução do serviço de treinamento, limitado a no máximo 30% (trinta por cento) do valor total do contrato, sem prejuízos das responsabilidades contratuais e legais da **CONTRATADA**.
- 13.2. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a **CONTRATADA**.
- 13.3. É vedada a subcontratação de empresa ou consórcio que tenha participado do processo licitatório do qual se originou a contratação.
- 13.4. As empresas de prestação de serviços técnicos especializados deverão garantir que os integrantes de seu corpo técnico executem pessoal e diretamente as obrigações a eles imputadas, quando a respectiva relação for apresentada em processo licitatório.
- 13.5. A **CONTRATADA** será, no caso de subcontratação, a única responsável pela plena execução do objeto contratado.



CLÁUSULA DÉCIMA QUARTA - DA FUSÃO, CISÃO E INCORPORAÇÃO

- 14.1. A fusão, cisão ou incorporação da **CONTRATADA** poderá ser admitida, desde que não prejudique a execução do contrato.

CLÁUSULA DÉCIMA QUINTA – DA GESTÃO DO CONTRATO

- 15.1. A gestão e a fiscalização do contrato consistem na verificação da conformidade da sua escorreita execução e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do pactuado, devendo ser exercido pelo gestor do contrato designado pela **SPTTrans**, que poderá ser auxiliado pelo fiscal técnico e fiscal administrativo do contrato, cabendo ao responsável legal ou preposto da **CONTRATADA** o acompanhamento dessas atividades.
- 15.2. As comunicações recíprocas deverão ser efetuadas por meio de correspondência mencionando o número do Contrato, o assunto específico do seu conteúdo e serem endereçadas conforme segue:

SPTTrans:

SÃO PAULO TRANSPORTE S/A. – Superintendência de Tecnologia – DG/STI
Responsável pela gestão do Contrato: Mauricio Lima Ferreira
Endereço eletrônico: mauricio.lima@sptrans.com.br

Fiscal técnico: Heitor Arantes Farres
Endereço eletrônico: heitor.farres@sptrans.com.br

Fiscal administrativo: Mauricio de Moraes
Endereço eletrônico: mauricio.moraes@sptrans.com.br

Endereço: Rua Boa Vista, 236 - 6º andar/meio – Centro - São Paulo/SP – CEP: 01014-000

CONTRATADA:

KRYPTUS SEGURANÇA DA INFORMAÇÃO S/A.

Responsável pela gestão do Contrato: André Schwartz Varejão – Gerente de Projeto - PMP

Endereço: Rua Maria Tereza Dias da Silva, 270 – Cidade Universitária – Campinas – SP - CEP: 13083-820

Endereço eletrônico: andre.varejao@kryptus.com

- 15.3. Quando for necessário, a entrega de qualquer carta ou documento far-se-á por portador, com protocolo de recebimento e o nome do remetente conforme acima descrito ou, ainda, por correspondência com Aviso de Recebimento – AR, endereçada conforme descrito nesse item.
- 15.4. As substituições dos responsáveis de ambas as partes, bem como qualquer alteração dos seus dados, deverão ser imediatamente comunicadas por escrito.

CLÁUSULA DÉCIMA DEXTA - DA TOLERÂNCIA

- 16.1. Se qualquer das partes contratantes, em benefício da outra, permitir, mesmo por omissão, a inobservância no todo ou em parte, de qualquer das cláusulas e



Y
Z

condições do presente contrato e/ou seus anexos, tal fato não poderá ser considerado como modificativo das condições do presente contrato, as quais permanecerão inalteradas, como se nenhuma tolerância houvesse ocorrido.

CLÁUSULA DÉCIMA SÉTIMA – CONDIÇÕES DE RECEBIMENTO

- 17.1. O Termo de Recebimento Provisório deverá ser lavrado, atendidas as condições previstas e cumpridas a totalidade do objeto contratual, dentro de 15 (quinze) dias, contados da data da comunicação escrita da **CONTRATADA**.
- 17.2. O termo de Recebimento Definitivo da prestação dos serviços deverá ser lavrado após 60 (sessenta) dias corridos, a contar da data de emissão do Termo de Recebimento Provisório.

CLÁUSULA DÉCIMA OITAVA - DO ENCERRAMENTO DO CONTRATO

- 18.1. Executada a prestação de serviço o contrato será encerrado lavrando-se o respectivo "Termo de Conclusão, Encerramento e Quitação", somente após a confirmação da inexistência de qualquer pendência impeditiva, seja operacional, financeira ou de qualquer outra natureza.
- 18.2. A emissão do "Termo de Conclusão, Encerramento e Quitação" não desobriga a **CONTRATADA** de cumprir o prazo de garantia do produto.

CLÁUSULA DÉCIMA NONA - DOS CASOS OMISSOS

- 19.1. A execução do presente contrato, bem como as hipóteses nele não previstas, serão regidas pela Lei Federal nº 13.303/16, legislação correlata e pelos preceitos de direito privado.

CLÁUSULA VIGÉSIMA – DAS DISPOSIÇÕES GERAIS

- 20.1. Para execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, nos termos do Decreto nº 56.633, de 24 de novembro de 2015.
- 20.2. A **CONTRATADA** declara que conhece e se compromete, no cumprimento do presente contrato, a respeitar as disposições contidas no Código de Conduta e Integridade da **SPTTrans** e suas atualizações.
- 20.3. Em cumprimento ao item 7 do Código de Conduta e Integridade da **SPTTrans**, os canais de denúncias relativas a às questões éticas e de integridade institucional são os seguintes:
e-mail: ouvidoria@sptrans.com.br
telefone: 3396-7853
correspondência: Envelope Lacrado endereçado a:
Comitê de Conduta da **SPTTrans**



Y
LG

Rua Boa Vista, nº 236 - 1º andar (Protocolo)

CLÁUSULA VIGÉSIMA PRIMEIRA - DO FORO

21.1. Elegem as partes contratantes o Foro Privativo das Varas da Fazenda Pública desta Capital, para dirimir todas e quaisquer questões oriundas deste contrato, renunciando expressamente a qualquer outro, por mais privilegiado que seja.

E, por estarem justas e contratadas, as partes, por seus representantes legais, assinam o presente Contrato, elaborado em 02 (duas) vias de igual teor e forma, para um só efeito jurídico, perante as testemunhas abaixo assinadas, a tudo presentes.

São Paulo, 01 de novembro de 2022.

SÃO PAULO TRANSPORTE S/A
"SPTTrans"

MAURÍCIO LIMA FERREIRA
Procurador

GEORGE WILLIAM GIDALI
Diretor de Gestão da Receita e
Remuneração

KRYPTUS SEGURANÇA DA INFORMAÇÃO S/A.
"CONTRATADA"

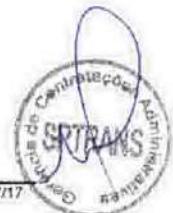
LEONARDO APARECIDO FIGUEIREDO
CABRAL
Diretor Administrativo e Financeiro

ROBERTO ALVES GALLO FILHO
Diretor Geral

Test
1ª _____
Nome: Carolina B.V. Francisco
CPF: _____

2ª _____
Nome: Keila Maria da Conceição Sileo
CPF: _____

CONTRATO registrado na
Gerência de Contratações Administrativas da
SÃO PAULO TRANSPORTE S/A em
01/11/22 sob n.º 2022/0281-01-00
Sonia Lima
PROM. 90.000,00
DA / SAM / GCA



ANEXO II
TERMO DE REFERÊNCIA



TERMO DE REFERÊNCIA

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, VARREDURA DE VULNERABILIDADES, TESTES DE INTRUSÃO/PENETRAÇÃO E GERAÇÃO DE RELATÓRIOS, PELO PERÍODO DE 60 (SESSENTA) MESES.

ITEM	ESPECIFICAÇÕES TÉCNICAS
1	Contratação de serviços gerenciados de segurança da informação, compreendendo o monitoramento de comportamentos que apresentem risco e vulnerabilidades em regime 24x7, suportar a SPTRANS no direcionamento do tratamento de incidentes de segurança, treinamento da equipe e suporte a implantação de boas práticas, pelo período de 60 (sessenta) meses.



Sumário

1. CONDIÇÕES GERAIS:.....	3
2. CARACTERÍSTICAS GERAIS	5
3. TERMOS E DEFINIÇÕES	6
4. SOLUÇÃO DE MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA.....	11
5. CARACTERÍSTICAS DO SERVIÇO DO SIEM	13
6. SOLUÇÃO PARA AUDITORIA, GESTÃO, AUTOMAÇÃO, MONITORAÇÃO E PREVENÇÃO DE AMEAÇAS INTERNAS E IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS EM DOCUMENTOS NÃO ESTRUTURADOS EXISTENTES NOS SERVIÇOS DO AD (MICROSOFT ACTIVE DIRECTORY), E SERVIDORES DE ARQUIVOS (MICROSOFT FILE SERVER)	30
7. SOLUÇÃO PARA VARREDURA DE VULNERABILIDADES	50
8. REQUISITOS TÉCNICOS DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES	52
9. SOLUÇÃO PARA AUTOMAÇÃO, GESTÃO, DESCOBERTA, IMPLEMENTAÇÃO E INVENTÁRIO DE PATCHES EM AMBIENTE DE SERVIDORES E ESTAÇÕES DE TRABALHO CONTEMPLANDO SISTEMAS OPERACIONAIS MICROSOFT E LINUX.....	55
10. DLP – DATA LOSS PREVENTION	63
11. DCS – DATA SECURITY EXTENDED	74
12. TESTE DE INTRUSÃO/PENETRAÇÃO	87
13. TESTES DE INVASÃO EM APLICAÇÕES WEB CONTINUO E RECORRENTE	93
14. SOLUÇÃO WEB APPLICATION FIREWALL (WAF).....	94
15. CONDIÇÕES PARA EXECUÇÃO DO TRABALHO	95
16. EXPERIÊNCIA EXIGIDA DA CONTRATADA.....	96
17. ACORDO DE NÍVEL DE SERVIÇO PARA DISPONIBILIDADE DA SOLUÇÃO DE ANÁLISE DE VULNERABILIDADE	97
18. NÍVEL DE SERVIÇOS	97
19. SUPORTE TÉCNICO DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES	98
ANEXO I.....	101



1. CONDIÇÕES GERAIS:

- 1.1. objetivo principal desta contratação é aumentar o nível de Segurança da Informação da SPTRANS através:
- 1.2. Monitoramento e gerenciamento de segurança em relação a comportamentos que apresentem riscos ao ambiente da SPTRANS;
- 1.3. Avaliações periódicas de falhas e vulnerabilidades de maneira recorrente;
- 1.4. Validação da aplicação das correções de varreduras anteriores, tornando-se assim um controle de qualidade sobre o processo de gestão de patches de infraestrutura e de aplicação;
- 1.5. Prover solução para automação, gestão, descoberta, implementação e inventário de patches em ambiente de servidores e estações de trabalho contemplando sistemas operacionais Microsoft e Linux.
- 1.6. DLP – Data Loss Prevention que consiste em um conjunto de políticas de segurança e regras que podem ser aplicadas com a ajuda de softwares especializados para reforçar o bloqueio contra possíveis invasores.
- 1.7. DCS – Data Center Security Extended que consiste em uma solução baseada no fortalecimento de segurança e monitoramento para nuvem privada e data centers físicos.
- 1.8. Execução de testes de intrusão recorrentes para desafiar a maturidade do processo, bem como abrangência e escopo dos controles estabelecidos no processo de gestão de vulnerabilidades, e consequentemente da gestão de patches;
- 1.9. Prover solução para detecção de explorações do sistema operacional, de forma a ser capaz de monitorar, em tempo real, todas as invocações a funções de sistema (syscalls) em ambiente Linux que possam ter relação com ações não autorizadas com foco em zero day.
- 1.10. Prover solução de auditoria, gestão, automação, monitoração e prevenção de ameaças internas e identificação e classificação de informações sensíveis



em documentos não estruturados existentes nos serviços do AD (Microsoft Active Directory), servidores de arquivos (Microsoft File Server)

- 1.11. Prover serviço de monitoramento da Surface, Dark e Deep Web sobre a marca da SPTRANS
- 1.12. Prover serviço de segurança baseado em Edge computing WAF.
- 1.13. Objetivo dessas ações é garantir a detecção de brechas e vulnerabilidades sistêmicas evitando que possam ser utilizadas por criminosos digitais para a prática de crimes, fraudes e/ou desvios de recursos econômicos/financeiros da SPTRANS, assessorar na solução das vulnerabilidades detectadas, implementação das melhores práticas de segurança da informação com base nas normas técnicas ABNT e ISO aplicáveis, na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), normas e orientações da Agência Nacional de Proteção de Dados – ANPD, no Guia de Boas Práticas para Implementação na Administração Pública Federal, editada pelo Comitê de Governança de Dados do Governo Federal em abril/2020, e no E-ping - Padrões de Interoperabilidade de Governo Eletrônico, com o objetivo de atender a Política Municipal de Governança de Tecnologia da Informação e Comunicação, prevista no Decreto nº 57.653/2017, do Município de São Paulo, e a Política de Segurança da Informação da SPTrans em todos os sistemas informatizados da SPTRANS.
- 1.14. A CONTRATADA deverá manter durante toda a vigência do contrato profissional(is) certificado(s), sendo que um mesmo técnico poderá deter mais de uma certificação, não devendo ser necessariamente um técnico para cada especialidade. São as certificações mínimas:
 - 1.14.1. Ethical Hacker, certificado oficial emitido por unidade certificadora EXIN ou equivalente;
 - 1.14.2. ITIL SERVICE MANAGEMENT FOUNDATION, certificado oficial emitido por unidade certificadora credenciada pela responsável pela certificação.



- 1.14.3. INFORMATION SECURITY MANAGEMENT ISSO/IEC 27001, certificado oficial emitido por unidade certificadora credenciada pela responsável pela certificação.
- 1.14.4. EXIN PRIVACY & DATA PROTECTION FOUNDATION, certificado oficial emitido por unidade certificadora, ou equivalente.
- 1.14.5. EXIN DATA PROTECTION OFFICER, certificado oficial emitido por unidade certificadora credenciada pela responsável pela certificação ou equivalente.
- 1.14.6. COBIT 5 FOUNDATION, certificado oficial emitido por unidade certificadora credenciada pela responsável pela certificação.

2. CARACTERÍSTICAS GERAIS

2.1. A solução deverá oferecer um Security Operations Center (SOC).

O SOC será um serviço de segurança para a infraestrutura de TI da SPTRANS em regime 24/7, a operação deverá ser remota, em localidade da contratada, protegendo a SPTRANS caso ocorra um incidente que possa afetar a segurança impactando a continuidade operacional de seus negócios.

Essa operação operará integrada com um conjunto de ferramentas, processos e equipe, no qual todas as ações de segurança serão centralizadas e dentro de um fluxo contínuo e correlacionado, de forma uniforme para a segurança esperada, sendo responsável por garantir que possíveis incidentes sejam corretamente identificados, analisados, defendidos, investigados e relatados.

O serviço de SOC deverá utilizar uma solução de SIEM/SOAR que irá monitorar e analisar as atividades nos servidores, bancos de dados, aplicativos, sites e outros sistemas, procurando atividades anômalas que possam indicar um incidente ou comprometimento da segurança.



2.2. O serviço também contemplará uma solução para varredura de vulnerabilidades, testes de intrusão, "phishing" testes como serviço – SaaS, Implantação, Manutenção, Relatórios e Treinamentos

A solução de análise de vulnerabilidades à ser adotada, as varreduras de vulnerabilidades do ambiente, os testes de intrusão, os testes de "phishing" e geração dos relatórios técnicos e executivos, objetos deste edital, irão proporcionar visibilidade e informações sobre como está a segurança de todo ambiente computacional da SPTRANS, possibilitando assim uma melhoria continuada do ambiente computacional, adotando boas práticas de segurança e aplicação das correções necessárias, garantindo assim um ambiente com maior segurança e consciência do que precisa ser melhorado e padronizado.

3. TERMOS E DEFINIÇÕES

3.1. IDOR: (Insecure Derect Object Reference) ocorre quando uma aplicação expõe uma referência a um objeto da aplicação interna. Usando dessa forma, ele revela o identificador real e o formato padrão usado do elemento no backend de armazenamento. O IDOR não traz um problema direto de segurança, pois, por si só, revela apenas o formato padrão utilizado para o identificador do objeto. O IDOR traz, dependendo do formato ou padrão em vigor, uma capacidade para o invasor e montar um ataque de enumeração para tentar sondar o acesso aos objetos associados.

3.2. EXPLOIT: Um exploit geralmente é uma sequência de comandos, dados ou uma parte de um software elaborados por hackers que conseguem tirar proveito de um defeito ou vulnerabilidade

3.3. Bug Chain: Falhas que possuem uma sequência que analisadas sozinhas podem ter baixo impacto mas em conjunto podem demonstrar um risco alto.



- 3.4. EPS: Volume de Eventos Por Segundo, processados que define a capacidade do processamento da ferramenta de correlação de eventos, normalmente denominada SIEM.
- 3.5. 0-day (dia 0): Uma vulnerabilidade de dia zero (também conhecida como dia 0) é uma vulnerabilidade de software de computador que é desconhecida para aqueles que estariam interessados em atenuar a vulnerabilidade (incluindo o fornecedor do software de destino).
- 3.6. Backdoors: Backdoor é um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas existentes em programas instalados, softwares e sistemas operacionais.
- 3.7. CIDR: O CIDR (de Class less Inter-Domain Routing), foi introduzido em 1993, como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos. O CIDR está definido no RFC 1519.
- 3.8. CIS: O Centro de Segurança da Internet (CIS) é uma organização sem fins lucrativos. Sua missão é "identificar, desenvolver, validar, promover e sustentar soluções de melhores práticas para defesa cibernética e construir e liderar comunidades para possibilitar um ambiente de confiança no ciberespaço.
- 3.9. CVE: Lista de entradas – cada uma contendo um número de identificação, descrição e pelo menos uma referência pública – para vulnerabilidades de cibersegurança publicamente conhecidas. As Entradas CVE são usadas em vários produtos e serviços de segurança cibernética de todo o mundo.
- 3.10. CVSS: O Common Vulnerability Scoring System (CVSS) fornece uma maneira de capturar as principais características de uma vulnerabilidade e produzir uma pontuação numérica que reflete sua gravidade.
- 3.11. CVSS BASE: O Common Vulnerability Scoring System (CVSS) fornece uma maneira de capturar as principais características de uma vulnerabilidade e produzir uma pontuação numérica que reflete sua gravidade. A pontuação numérica pode então ser traduzida em uma representação qualitativa (como

baixa, média, alta e crítica) para ajudar as organizações a avaliar e priorizar adequadamente seus processos de gerenciamento de vulnerabilidades.

- 3.12. **Exploits:** (português explorar), pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento accidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico (normalmente computadorizado). Tal comportamento frequentemente inclui coisas como ganhar o controle de um sistema de computador, permitindo elevação de privilégio ou um ataque de negação de serviço
- 3.13. **HOST:** Em informática, host ou hospedeiro, é qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede.
- 3.14. **LDAP:** Lightweight Directory Access Protocol, ou LDAP, é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP).
- 3.15. **Malwares:** Um código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso (em inglês: malware, abreviação de "malicious software").
- 3.16. **Netbios:** NetBIOS é um acrônimo para Network Basic Input/Output System, ou em português Sistema Básico de Entrada/Saída de Rede. É uma API que fornece serviços relacionados com a camada de sessão do modelo OSI, permitindo que os aplicativos em computadores separados se comuniquem em uma rede local.
- 3.17. **OVAL:** Open Vulnerability and Assessment Language esforço comunitário internacional de segurança da informação para promover conteúdo de segurança aberto e publicamente disponível e para padronizar a transferência dessas informações por todo o espectro de ferramentas e serviços de segurança.
- 3.18. **OWASP:** O OWASP (Open Web Application Security Project), ou Projeto Aberto de Segurança em Aplicações Web, é uma comunidade online que cria e

disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.

- 3.19. **Patch Tuesday:** O termo Patch Tuesday é um pacote de atualizações da Microsoft para os seus produtos. Estes pacotes vêm pelo Windows Update atualmente, e são lançados em todas as segundas Terça-Feira de cada mês
- 3.20. **PCI:** O PCI Security Standards Council é um fórum aberto global para o contínuo desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados de contas.
- 3.21. **PCI ASV:** PCI (Payment Card Industry) ASV (Vendedor de Verificação Aprovado). Um ASV é uma organização com um conjunto de serviços e ferramentas de segurança (solução de varredura ASV) para conduzir serviços externos de varredura de vulnerabilidades para validar a conformidade com os requisitos de varredura externa do PCI DSS.
- 3.22. **PCI DSS:** O PCI DSS, acrônimo para Payment Card Industry Data Security Standards (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento), é um padrão que prevê a proteção da privacidade e da confidencialidade dos dados de cartões de pagamento.
- 3.23. **Peer to peer:** (do inglês peer-to-peer, que significa par-a-par) é um formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo.
- 3.24. **PHISHING:** Phishing é o termo que designa as tentativas de obtenção de informação pessoalmente identificável através de uma suplantação de identidade por parte de criminosos em contextos informáticos (engenharia social).
- 3.25. **PROXY:** proxy (em português 'procurador', 'representante') é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Um cliente conecta-se ao servidor proxy, solicitando algum serviço, como um arquivo, conexão, página web ou outros recursos disponíveis de um servidor

diferente, e o proxy avalia a solicitação como um meio de simplificar e controlar sua complexidade.

- 3.26. **SANS:** A SANS – System Administration, Networking and Security (oficialmente Escal Institute of Advanced Technologies) é uma empresa privada norte-americana especializada em segurança da informação e treinamento de cybersegurança. Juntamente com a Nacional Infrastructure Protection Center (NIPC), elabora anualmente a SANS Top-20, um documento que lista as 20 vulnerabilidades de segurança mais críticas da internet, como perigos para os sistemas operacionais Windows e Unix. As falhas nos sistemas operacionais e programas em geral permitem invasão e manipulação de computadores por meio de ataques diversos, incluindo vírus, worms e cavalos de Tróia.
- 3.27. **SCAP:** O SCAP (Security Content Automation Protocol) é um método para usar padrões específicos para permitir o gerenciamento automatizado de vulnerabilidades, a avaliação e a avaliação de conformidade de políticas de sistemas implantados em uma organização.
- 3.28. **SCCM:** O System Center Configuration Manager (SCCM) é um componente da configuração do centro de sistemas da Microsoft para plataformas de servidor e cliente. Ele permite que profissionais administrativos ajudem os usuários finais a obter acesso aos dispositivos e aplicativos de que precisam sem comprometer a segurança corporativa.
- 3.29. **SIEM:** Gerenciamento e Correlação de Eventos de Segurança (em inglês Security Information and Event Management), permite que os eventos gerados por diversas aplicações de segurança (tais como firewalls, proxies, sistemas de prevenção a intrusão (IPS) e antivírus sejam coletados, normalizados, armazenados e correlacionados; o que possibilita uma rápida identificação e resposta aos incidentes
- 3.30. **SLA:** Um Acordo de Nível de Serviço (ANS), Contrato de Nível de Serviço ou Garantia do Nível de Serviço (i.e. SLA, do inglês Service Level Agreement) é um compromisso assumido por um prestador de serviços de TI perante um cliente.



- 3.31. SNMP: Simple Network Management Protocol (SNMP), em português Protocolo Simples de Gerência de Rede, é um "protocolo padrão da Internet para gerenciamento de dispositivos em redes IP".
- 3.32. Trojans: tipo programa malicioso que podem entrar em um computador disfarçados como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de forma que usuários mal-intencionados possam invadir um determinado software e/ou sistema operacional.
- 3.33. Virtual Appliance: Um Virtual Appliance é uma máquina virtual pré-criada, normalmente para um fim específico e com um aplicativo específico.
- 3.34. WSUS: Windows Server Update Services (WSUS), anteriormente conhecido como Software Update Services (SUS), é um programa de computador desenvolvido pela Microsoft Corporation que permite aos administradores gerenciar a distribuição de atualizações e hotfixes lançados para produtos da Microsoft para computadores em um ambiente corporativo.

4. SOLUÇÃO DE MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA

- 4.1. Deverá prever a implementação de um "SOC" (Security Operation Center), em regime ininterrupto (24x7x365), para monitoramento da infraestrutura interna da SPTRANS sobre o escopo de segurança da informação, com foco em detecção de comportamento anormal abrangendo Banco de Dados, Dispositivos, Aplicação, Link, Servidores, Segurança da Infraestrutura e Banco de Dados. Os detalhes desses itens estão apresentados no anexo I;

- 4.2. Monitoramento externos, ambiente WEB.

Monitoramento de repositórios públicos (pastebin, github, etc.) visando detectar informações confidenciais e forma pública, como trechos de código fonte, logins e senhas etc;

Detecção de sites de phishing ou que personificam a marca da SPTRANS e tentativa de eliminação;

Monitoramento em todas as camadas da WEB (surface, deep e dark-web) para



- detecção de possíveis ameaças e/ou vazamentos;
- Monitoramento de uso indevido ou fraudulento da marca;
- Monitoramento de domínio similares para execução de fraude;
- Monitoramento de aplicativos falsos e disponibilizados em lugares como Google Play e Apple Store;

4.3. Monitoramento internos e testes.

- Avaliações em endpoints com antivírus da SPTRANS medindo a segurança;
- Avaliação da segurança em redes e Wifi;
- Varredura automática de ativos;
- Scanner de vulnerabilidades Web (DAST), deverá ter dashboard de acompanhamento e comparativo da evolução da segurança, permitir a análise e re-execuções por demanda.
- Baseline e conformidade dos ativos (hardening);
- Ataques físicos contra a infraestrutura da SPTRANS;
- Ataques físicos de engenharia social na infraestrutura da SPTRANS;
- Analizar, tratar e responder aos eventos e incidentes de segurança cibernética, oriundos de ferramentas de monitoração e detecção de ataques, relatórios técnicos, e-mails, usuários e outros canais de entrada, inclusive externos;
- Investigação forense digital, como de pessoas (fraudadores, crackers etc.) ou de sistemas computacionais e de redes de dados, como também outros serviços forenses que envolvam obtenção de evidências materiais e não materiais (como de computadores, unidades de armazenamento de dados e redes de comunicação de dados) visando identificar fraudes e golpes praticados contra SPTRANS;
- Realizar respostas aos incidentes cibernéticos decorrentes de vulnerabilidades sistêmicas;
- Vigilância de meios de comunicação e análise de dados dos crackers e fraudadores;
- Realizar a comunicação com outros CSIRT's, órgãos como CERT.br, CTIR, NIC, USCERT, entre outros, quando necessário;



Prover todos os alertas possíveis assim como recomendações para solução de falhas de "dia-zero"

Avaliação das políticas de backup;

4.4. Treinamento

Deverá ser proposto um plano com conteúdo para uma palestra sobre segurança cibernética visando melhorar a cultura de segurança da SPTRANS, esse plano terá como entregável, Conteúdo que será disponibilizado a SPTRANS, Proposição de cronograma, Teste de absorção e indicação. Deverá ocorrer a cada 6 meses tendo como público os técnicos indicados pela SPTrans no limite máximo de 35 pessoas visando transmitir as melhores práticas de segurança.

4.5. Recursos internos

Para a prestação de serviço deverá prever 1 (hum) recurso como gestor da qualidade das entregas da operação para coordenar o alinhamento com os interlocutores locais da SPTRANS conforme a necessidade para ajustar os entregáveis.

5. CARACTERÍSTICAS DO SERVIÇO DO SIEM

5.1. Os componentes da solução de SIEM deverão permitir a realização das seguintes funções e características:

5.1.1. Arquitetura Básica

A solução de segurança proposta deverá ter a descrição se será de um único fabricante de modo que tanto o suporte da solução, quanto as funcionalidades sejam integradas e 100% compatíveis ou se utilizará várias plataformas, neste caso como garantirá a integração.

A prestação dos serviços deve ser feita de forma centralizada sem complexidade para obter informação;



A solução deverá ser fornecida para instalação e uso no idioma Português Brasil (pt br);

A solução deverá ter o pleno funcionamento independentemente de outros recursos não descritos na arquitetura descrita nesta proposta;

A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante;

A solução deve sincronizar o horário de seus componentes utilizando o serviço NTP ou RDate da SPTRANS;

A solução deve ser gerenciada centralmente e remotamente (configurações, controle e atualizações), através de interface web única, sem necessidades de intervenção nos equipamentos onde está instalada;

A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar os ativos descritos no anexo 1, o volume de 7.500 EPS estimados no qual a solução deverá suportar;

A solução deve permitir a recepção de eventos que excedam temporariamente os limites contratados em até 10% no limite de até 2 horas mensais, processando o volume excedente assim que volume for normalizado. Mantendo a operação com situações de picos temporários, sem incorrer na perda de eventos e sem incorrer em: qualquer cobrança adicional por excesso ou bloqueio da solução.

Os componentes da solução de Console, Coletor, Correlacionador e armazenamento de logs devem ser fornecidos em Alta-disponibilidade, ou seja, mesmo com a falha de um dos componentes da solução, toda a solução deve continuar funcionando, sem a necessidade de intervenção manual;

Ao utilizar de mais de um componente na solução, a comunicação deverá ser feita de forma criptografada quando necessário, garantindo a autenticidade, confidencialidade e integridade dos dados;

Qualquer acesso deve ser feito de forma segura;

Ter suporte a monitoração a partir SNMPv2c ou versões posteriores.

A solução deve prover aceleradores de implementação, boas práticas e



aumento da inteligência e funcionalidades através de integrações adicionais e aplicações de terceiros, em formato de plug-in ou "App".

A solução deve possuir um SDK para criação de novos Apps/Plugins, de forma a permitir que possa desenvolver aplicações e extensões livremente.

A solução por motivo de rastreabilidade a administração da solução deve usar uma única conta para cada usuário administrador (mesma conta, mesma senha), independente da funcionalidade gerenciada.

5.1.2. Processamento Interno nas dependências da SPTRANS

Caso seja necessário deverá ser fornecido no formato de máquina virtual, configurado especificamente para atender a solução, acompanhado do sistema operacional (software) otimizado para esse fim a ser implantado nas dependências da SPTRANS para a coleta dos dados.

Descrever os requisitos da máquina virtual na proposta para que a SPTRANS possa prever os recursos computacionais em seu ambiente.

5.1.3. Tratamento de eventos

A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real;

Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução;

A solução para facilitar a geração da informação deverá permitir a definição de metadados customizados/personalizados, para extrair dados existentes na linha de log (raw), usando recursos como expressões regulares ou algum recurso gráfico para essa extração.

A solução deve permitir a agregação de eventos semelhantes para a melhor entrega e tomada de decisão;

O SIEM deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;

Gerar alertas/incidentes com base nas regras definidas previamente;



Verificar conformidade com as políticas, controles e normas internas (personalizadas) e regulamentações externas tais como (ex. ISO 27001, PCI, HIPAA);

Deverá ser fornecido uma interface para o gerenciamento dos incidentes identificados pela solução.

Ter facilidade para gerar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema do SIEM, garantindo a qualidade dos seus serviços;

O Siem como solução deve permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;

Permitir a visualização para a equipe do SOC do prestador, na interface da aplicação, dos eventos relacionados a um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução;

Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog;

A solução deverá ter, no mínimo, as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v2 e v3), Microsoft Event Log, Arquivos de Log em formato de texto, Kafka, AWS Cloudwatch, Checkpoint OPSEC/LEA, CISCO NSEL e Juniper NSM Protocol;

A solução deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados;

A ofuscação de dados deve ser configurada com chaves de criptografia;

Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação.

Possuir a capacidade de customizar e personalizar diferentes "templates" de e-mail que serão enviados como resposta aos incidentes identificados.

Deve ser capaz de processar logs em formatos JSON, CEF e LEEF,



identificando e criando automaticamente os campos comuns do log como metadados para aqueles tipos de log.

Deve ser capaz de processar logs em formato JSON permitindo a definição manual/customizada de metadados, usando a estrutura/caminho do JSON para a definição da propriedade.

A solução deve permitir a definição de metadados customizados e personalizados, para extrair dados de uma linha de log (raw), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, permitindo usar esses dados em pesquisas de eventos.

5.1.4. Coleta de logs

A coleta de logs deve permitir filtrar e selecionar os eventos que serão inseridos na solução ou que serão retidos na base de dados da solução por períodos previamente definidos. Deve permitir a criação e alteração de políticas de retenção;

Normalizar e categorizar os eventos em um padrão único que será usado pela solução;

Possuir suporte nativo, suportado pelo fabricante, para coleta, reconhecimento e normalização de pelo menos, 350 tipos de fontes de dados logs;

Tratar eventos em formato “comprimido” (zip, gz, tar.gz), sem a necessidade da descompressão manual;

Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado;

Deve manter o evento bruto (“raw”) e seus metadados para o armazenamento e consulta futura;

Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;

A solução deve permitir a integração de dispositivos ou logs não suportados nativamente;

A integração de logs ou dispositivos deve permitir em caso de necessidade ser realizada, com o uso de expressões regulares, JSON e recurso similar, sem exigir o uso de linguagens de programação ou scripts, tais como Java, C, TCL/TK, PowerShell, Shell Scripts, etc.

A mesma integração deve suportar as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, Arquivos de Log em Formato de texto, Check Point OPSEC/LEA, CISCO NSEL, Kafka, Juniper NSM Protocol.

A solução deve suportar, nativamente, pelo menos as seguintes fontes de logs: Windows, Linux, Oracle Database, MS SQL Server, Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet e watchguard), Network IPS (Pelo menos 3 fornecedores compatíveis);

A solução do SIEM deve permitir a criação automática ou com facilidade, para que novos data sources possam ser adicionados pela detecção do tipo de fonte do log, dentre as nativamente suportadas, enviados via Syslog

A solução deve suportar "overlap de IP", isto é, rotular os eventos para que seja possível gerenciar eventos de fontes de log que estejam em redes diferentes, mas possuem o mesmo endereçamento IP.

5.1.5. A solução de SIEM quanto ao Correlacionamento

Deve permitir tratar logs e flows em conjunto, gerando incidentes de segurança;

Efetuar o correlacionamento dos eventos próximo ao tempo real;

A solução deve estar dimensionada e licenciada para correlacionar os eventos coletados e normalizados conforme a tabela de ativos;

Deve permitir a criação de novas regras e a edição das existentes;

Deve permitir o correlacionamento de qualquer informação que conste no evento, inclusive informações que não sejam referentes a endereçamento IP, portas, etc, tais como dados financeiros;



Descrever se suporta o mínimo 350 regras de correlação online, especializadas na detecção de incidentes de segurança, produzidas, suportadas e atualizadas pelo fabricante da solução;

Deve possuir regras de correlação específicas para regulações/conformidades, com suporte no mínimo a: PCI, ISO 27001 e GDPR/LGPD;

Deve possuir repositório do fabricante da solução que ofereça novas regras de correlação especializada em segurança para atualização e ampliação da capacidade de detecção de incidentes, sem custo adicional;

Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);

Deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e não foram previstos ou observados anteriormente;

Integrar com ferramentas externas de diagnóstico padrão tais como: Nslookup, Whois, Nmap;

Permitir o correlacionamento de eventos e alertas com dados existentes em listas (watchlist), permitindo também a criação de novas listas e a edição das existentes, de forma automatizada e manual;

Correlacionar eventos oriundos de mais de uma fonte, tipo ou localização;

Priorizar os eventos e incidentes com base, pelo menos, nos seguintes critérios: severidade e criticidade/relevância do evento ou incidente.

Podendo ser utilizada uma combinação desses critérios;

Os incidentes devem ser agrupados, no mínimo, por: categoria, endereço de origem, endereço de destino;

Possuir pelo menos os seguintes tipos de correlação:

Correlação por regras;

Correlação por anomalia e padrão de comportamento;

Como resultado das regras, deve ser capaz de executar ações



automáticas de comunicação, no mínimo: enviar e-mail, enviar mensagem para o usuário do SOC conectado no console, ser capaz de automatizar um incidente no sistema de workflow interno, enviar traps SNMP e popular listas (watch list);

Integrar-se com pelo menos um ou mais sistemas de inteligência com informações de riscos globais tais como: HP ThreatLink (DV Labs), Symantec DeepSight, Verisign iDefense, IBM X-Force;

Disponibilizar pelo menos uma base de inteligência em ameaças com informações de riscos globais, com updates diários, integrada às regras de correlação para detecção de incidentes;

Qualquer metadado dos eventos pode ser usado em uma regra de correlação.

Deve permitir testar as regras de correlação em eventos passados, em período e escopo bem definidos.

Deve permitir usar as regras de correlação aplicada de forma histórica, em eventos já mantidos na base de dados da solução, sem afetar a execução das regras online. Deve permitir especificar qual horário a ser utilizado para a correlação, o da recepção do evento na solução ou o horário existente no evento/log.

A correlação histórica deve permitir a escolha do período a ser analisado, atendendo no mínimo a correlação compreendendo a análise de 1 dia, 7 dias e 30 dias.

Regras de correlação histórica devem processar gerando alertas quando os eventos analisados combinarem com o especificado na regra.

Uma regra de correlação deve ser capaz de correlacionar eventos de tipos diferentes, de origens diferentes, checando situações como: a ocorrência de uma sequência de diferentes eventos, uma contagem de eventos, a não ocorrência de um evento após a ocorrência de outro.

Mecanismo para ajuste fino de regras de correlação, exibindo de forma gráfica as regras de correlação que são mais acionadas por eventos (que geram mais alertas) e seus elementos relacionados. Facilitando o

refinamento da solução com vistas à redução de falso-positivo e melhoria da performance;

Dentre as regras de correlação fornecidas e suportadas pelo fabricante, deve possuir regras que a partir dos diversos tipos de logs, cubram os seguintes Casos de Uso:

Exfiltração de dados, detectando no mínimo o acesso a quantidade excessiva de arquivos, arquivos sensíveis sendo transferidos para host remoto ou malicioso, grande transferência de dados para endereço malicioso;

Apoiar na identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados) ou GDPR (General Data Protection Regulation)

Geração de incidente/alerta quando o alvo de um ataque é vulnerável ao ataque efetuado;

Comunicação da equipamentos internos com sites conhecidos por serem controladores de botnet

Identificação de servidor de e-mail da SPTRANS enviando e-mails para servidor categorizado como SPAM

Detecção de ações relacionadas à mineração de moedas digitais;

Monitoração de serviços de nuvem, detectando no mínimo: atividades de administração do serviço de nuvem efetuas com usuário com poderes totais (root/administrator), parada/terminação de instâncias de computação críticas, usuário adicionado a papel de administrador, auditoria do serviço de nuvem desabilitado;

5.2. Armazenamento de dados

Armazenar os dados: eventos, flows, incidentes, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria;

Deve armazenar os eventos e flows de acordo com política de retenção, sempre comprimidos, e excluídos após um período definido de até 6 meses.

Deve armazenar os eventos em formato original ("raw") em conjunto com



propriedades normalizadas e outros metadados, de forma a permitir a pesquisa e visualização;

Armazenar logs por tempo determinado e customizado;

Deve permitir o uso de algoritmo para garantia de integridade dos eventos armazenados, utilizando no mínimo os algoritmos: MD2, MD5, SHA-256, SHA-384 e SHA-512;

Deve permitir o uso dos algoritmos para garantia de integridade, do item anterior, com código de autenticação da mensagem (HMAC).

Caso seja necessário deve possuir funcionalidade para expandir a capacidade de armazenamento de dados da solução, sem necessidade de reconstruir a base de dados, garantindo a integridade da solução;

Deve permitir o expurgo de eventos (metadados e raw) de forma automática, permitindo a customização do período de expurgo por diversos fatores, no mínimo: tipo/nome do evento e dispositivo/fonte de log;

Deve registrar todas as interações dos usuários e administradores com a solução em trilhas de auditoria.

A solução deve possuir funcionalidade de backup integrada, que faça a cópia de segurança de: eventos, flows, incidentes e demais dados, além das configurações;

Possuir mecanismos automatizados para backup dos dados em mídias off-line. Os dados serão mantidos por até 6 meses de forma off-line.

A solução deverá permitir a recuperação dos dados armazenados de forma off-line, e reinserção como dados online, isto é, quando necessário ser possível recuperar os dados armazenados em mídias off-line, e através de processos documentados reinseri-los na base de dados online para buscas, relatórios e investigações forenses.

Possuir mecanismo para detecção de abuso de domínios da Internet, detectando no mínimo: Tunelamento e domínios maliciosos gerados por algoritmos. Deve usar informações provenientes de logs de DNS e proxy, podendo também usar informações extraídas do tráfego de rede, quando disponível.

Deve ter a capacidade de armazenar todo os dados coletados de forma online por até 6 meses, isto é, podendo esses dados serem utilizados de forma imediata para buscas, relatórios e correlação histórica de eventos e flows rede.

5.3. Gerenciamento e Operação

Possuir acesso controlado e autenticado por usuário;

Possuir acesso seguro e criptografado à interface web, de forma a garantir a confidencialidade;

Garantir acesso aos dados e às funcionalidades/ações diferenciadas por perfis de acesso;

O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução a perfis de usuários, conforme critérios definidos pelo administrador;

O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, acesso a atividades de Redes e Logs;

Permitir visualização de eventos e incidentes de segurança em tempo próximo ao real;

Permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de "drill-down", ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa.

Deve permitir a visualização dos detalhes dos eventos, inclusive o evento original ("raw"), quando aplicável, para análise forense e investigação de incidentes;

Permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução;

Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;

Capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (ex: Firewall, Proxy e antivírus na mesma visualização);

Permitir a criação de novos modelos de relatórios e alteração dos relatórios nativos da solução sem a necessidade de uso de linguagens de programação,

através da interface web;

Permitir agendar a geração de relatórios de forma periódica e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

Capacidade de criação de listas (watchlist) e alteração das existentes.

Permitindo a inserção dos dados de forma manual, por linha de comando, por API ReST e automática através das regras de correlação;

Permitir a remoção de dados das listas (watchlist) de forma manual, automática através de regras de correlação, por API ReST e pela expiração do tempo de vida da informação;

Capacidade de gerenciamento e configuração centralizada de todas as partes distribuídas da solução;

Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente;

Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes, ou aos definidos pelo usuário;

Deve disponibilizar APIs do tipo webservices, do tipo "RESTful API", para acesso externo e integração com a solução, permitindo busca de informações de eventos e flows, manipulação de incidentes e uso de administração da solução;

Deve possuir templates de relatórios para as principais normas de conformidade. Sendo exigido, no mínimo, o atendimento a ISO/27001 e PCI;

A solução deve implementar auto monitoração, para detectar comandos que possam modificar arquivos de logs, tentativas de logins por força bruta, edição e remoção de arquivos sensíveis ou críticos da solução e o uso de contas compartilhadas de administradores da solução;

5.4. Tratamento de Incidentes

Possuir componente para o de tratamento dos incidentes identificados pelas regras de correlação;

Permitir associar os incidentes aos usuários da solução;



- Permitir encerrar um incidente quando este for solucionado;
- Permitir adicionar anotações aos incidentes para registro das ações tomadas ou observações;
- Permitir a manipulação dos incidentes identificados pela solução usando a API ReST, permitindo adicionar anotações, identificar os detalhes do incidente e encerrar o incidente usando esse acesso;
- Deve possuir integração suportada na solução, com ferramenta especializada no tratamento de resposta à incidente;
- Permitir a integração com ferramentas de tratamento de incidentes externos, nativamente ou possuir recursos como envio de Trap SNMP, Syslog e mensagens SMTP a partir da geração de um incidente, permitindo a manipulação do incidente.

5.5. Compatibilidade e escalabilidade

- A solução deverá executar sobre ambiente virtual, vmware e ou hyper-V.
- O componente de coleta de eventos deve suportar a recepção, a normalização, e o tratamento de eventos/logs em tempo próximo ao real (near real-time);
- A solução deve ter a capacidade para suportar a adição de novos componentes para garantir a escalabilidade, inclusive referente ao banco de dados;
- Os ativos indicados abaixo devem ser suportados pela solução, os quais poderão ter suporte nativo ou por meio de customização para coleta dos logs e correlação:

A lista abaixo representa equipamentos existentes e ou que podem ser adquiridos pela SPTTrans ou seus fornecedores de serviço:

- o Firewall:
 - Checkpoint;
 - Cisco ASA;
 - Cisco FirePower;
 - Fortinet Fortigate;



- Palo Alto Networks;
- IPTables;
- Watchguard
- Detecção/Prevenção de Intrusos/Anti-DDoS
 - Sourcefire Defense Center;
 - Snort;
 - Cisco IPS;
 - Radware DefensePro;
- Antivírus/Antimalware
 - Trend Micro;
 - Symantec System Center;
 - Symantec Endpoint Protection;
 - McAfee ePolicy Orchestrator (ePO);
 - Kaspersky Security Center;
 - FireEye;
 - F-secure
- Sistemas Operacionais
 - Linux;
 - Microsoft Windows;
- Servidor Web e Proxy
 - Microsoft IIS;
 - Apache;
 - NGinX Proxy Reverso;
 - Squid Web Proxy;
 - Websense
- Roteadores/switches



- 3com;
 - Nortel;
 - Extreme;
 - Enterasys;
 - Cisco;
 - Juniper;
 - Aruba;
- Servidor de Banco de dados e Ferramentas de DAM
 - Oracle;
 - Microsoft SQL
 - MongoDB;
 - Scanners de vulnerabilidades
 - Nessus;
 - QualysGuard;
 - Foundstone;
 - NMAP;
 - Concentrador VPN;
 - NORTEL;
 - Check point UTM;
 - Cisco;
 - Serviços em Nuvem
 - Amazon AWS CloudTrail
 - Amazon VPC Flow
 - Amazon GuardDuty
 - Microsoft Azure



5.6. Comportamento de usuário.

O módulo de análise de comportamento de usuário deve ser licenciado para processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM, quando aplicável, ou devem considerar o total de contas monitoradas (contas de usuários + contas de serviços).

Deve integrar nativamente com a solução de SIEM e ser capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco.

Deve ser capaz de importar dados de usuário em bases LDAP, CSV e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail e cargo.

O modelo de análise de comportamento do usuário usando modelos de Machine Learning, deve abranger a análise/retenção dos dados no mínimo por 30 dias, permitindo uma análise abrangente do usuário.

Deve permitir selecionar usuários que não devem fazer parte da análise com modelos de Machine Learning.

Permitir a criação de listas de observação com os principais usuários sob monitoração.

Deve possibilitar a inclusão de usuários nas listas de observações selecionando aqueles já existentes na solução que combinem com uma expressão regular ou similar.

Deve permitir a isenção de determinadas identidades do processo de score de risco. Essas identidades não teriam riscos computados relacionados as suas



atividades.

Deve permitir a inclusão de anotações dentro da monitoração de cada identidade com o objetivo de melhor gerenciamento de risco e do histórico e ações tomadas.

Deve possuir dashboards dos usuários com maior pontuação de risco e realizar um drill down para entender quais as categorias de risco e as ações que contribuíram para o score atual.

Deve permitir ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou precisam ser monitoradas.

A monitoração de desvios de comportamento de usuário deve detectar no mínimo:

- Tentativa de acesso a contas suspensas;
- Acesso negado repetido;
- Usuário acessando a VPN a partir de uma localidade atípica;
- Usuário acessando a VPN a partir de horários atípicos;
- Conta utilizada numa quantidade atípica de atividades;
- Acesso a máquinas Linux e Windows com contas de serviço;
- Primeiro uso de um recurso importante por um usuário;
- Acesso a endereços considerados suspeitos por bases de Threat feed/IP Reputation
- Detecção de comandos em blacklist por um usuário
- Conta de usuário criada em deletada rapidamente
- Detecção de ataque de negação de serviço pela deleção de contas
- Conta anômala criada a partir de uma nova localização



- Conta anômala em Cloud, criada a partir de uma nova localização
- Detecção de comportamento de Ransomware
- Compliance para General Data Protection Regulation (GDPR) ou Lei Geral de Proteção a Dados (LGPD)
- Deve ser capaz de aprender de forma supervisionada ou não supervisionada os comportamentos dos usuários;
- Uso de LDAP/AD para análises de definição de grupos de usuários que deverão ser analisados como "Peer Groups" por algoritmos de machine learning

6. SOLUÇÃO PARA AUDITORIA, GESTÃO, AUTOMAÇÃO, MONITORAÇÃO E PREVENÇÃO DE AMEAÇAS INTERNAS E IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS EM DOCUMENTOS NÃO ESTRUTURADOS EXISTENTES NOS SERVIÇOS DO AD (MICROSOFT ACTIVE DIRECTORY), E SERVIDORES DE ARQUIVOS (MICROSOFT FILE SERVER)

Fornecimento de solução de auditoria de dados não estruturados para o monitoramento das seguintes soluções que fazem parte do ambiente da SPTRANS:

- Auditoria para serviços de diretório (Microsoft Active Directory), têm por objetivo, de forma proativa e recorrente, identificar modificações no ambiente do Active Directory (AD), utilizado na SPTRANS para a criação de usuários e grupos de acesso e distribuição e concessão de permissionamento em serviços de rede Windows, Linux, controle de acesso a sistemas e bases de dados e documentos nas estruturas de compartilhamento de arquivos, além de acesso via Virtual Private Network (VPN), disponibilizado aos servidores da SPTRANS para a execução de trabalho remoto. Tal ferramenta visa também o monitoramento de uso fora do padrão para a identificação prévia de possíveis vetores de ataque aos dados da SPTRANS.
- Auditoria para serviços de compartilhamento de arquivos de redes, que visa mapear as permissões existentes para cada usuário e grupo de acesso nos



diretórios existentes nos compartilhamentos de rede disponíveis no ambiente da SPTRANS, com o intuito de avaliar permissões indevidas a dados sensíveis que poderão ser avaliados em conjunto com os donos destes dados. Tem por objetivo também identificar acessos mantidos por movimentações laterais dos usuários nas áreas, a redução dos acessos concedidos aos usuários e grupos de rede e a identificação proativa de comportamentos inesperados para o bloqueio de ataques, como o sequestro de informações (ransomwares).

6.1. CONSIDERAÇÕES GERAIS:

A solução deverá fazer o monitoramento e auditoria dos usuários e seus acessos internos e externos ao diretório de usuários, pastas, arquivos.

O monitoramento e auditoria deverão gerar indicadores de performance para a gestão dos dados não estruturados, de forma que a CONTRATANTE possa evoluir e melhorar a performance, capacidade e segurança das informações e dos recursos monitorados.

Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo deverá ser executado de forma a diminuir o impacto sobre a disponibilidade dos serviços.

Devido à complexidade e à quantidade de servidores monitorados, todas as informações e plataformas monitoradas deverão ser apresentadas em uma única console integrada que atenda aos requisitos deste termo de referência e que deve ter seu acesso controlado por meio de autenticação baseada em usuários do domínio da SPTRANS.

Deve ser possível a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o



acesso de analistas, equipe de suporte e usuários finais.

A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica.

A solução deve permitir o acesso a, no mínimo, 5 (cinco) anos de dados de auditoria capturados e armazenados.

A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização Vmware ou Microsoft Hyper-V.

Como a quantidade de servidores de arquivos, servidores de bancos de dados e controladores de domínio é variável, a solução deve ter escalabilidade para atender a quantidade crescente de servidores monitorados, sem a necessidade de aquisição de novas licenças.

Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade de as informações serem utilizadas para perícia, a solução deverá ter possuir evidências em formatos de relatórios para certificação são como a ISO/IEC 27.001 ou similares.

As soluções fornecidas pela contratada devem contemplar a auditoria de sistemas na última versão disponibilizada pelo fabricante.

As soluções fornecidas devem permitir auditar, controlar, monitorar e gerenciar as contas dos colaboradores.

A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos (Word, Excel,



PDF, CSV e XML), exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.

Deve ser possível, através da console, a criação de modelos de relatórios para posterior reutilização. Essa criação de modelos deve ser intuitiva e não deve necessitar da utilização de linguagem de programação ou outro software.

A documentação relativa às especificações técnicas da solução de TI deve ser fornecida em português. Alternativamente, poderá ser apresentada em Língua Inglesa.

A solução deve permitir o acesso de, pelo menos, 10 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que eventualmente sejam disponibilizadas a todos os usuários da SPTRANS, a solução deve permitir o acesso de todos os usuários.

A solução deve possuir interface nos idiomas português ou inglês.

Todos os itens apresentados nesta especificação são obrigatórios e deverão ser atendidos de forma nativa. Entende-se por itens atendidos de forma nativa, todos aqueles itens atendidos diretamente pelo software e seus módulos, sem a necessidade de alteração do código fonte em sua estrutura.

6.2. CARACTERÍSTICAS DE PERMISSIONAMENTO

A solução deverá apresentar, em sua interface, todos os usuários e grupos de segurança dos diferentes domínios monitorados, assim como os usuários e grupos de segurança locais de cada servidor ou plataforma monitorada.



A solução deve permitir a busca por uma pasta nos servidores monitorados e apresentar quais usuários e grupos de segurança têm permissões e quais permissões esses objetos têm na pasta.

A solução deverá consolidar as permissões NTFS e de compartilhamento de cada pasta e demonstrar a permissão efetiva dos usuários e grupos.

A solução deve utilizar os eventos coletados pela auditoria para realizar a análise comportamental dos usuários de maneira a permitir a geração de relatórios para revogação de acesso aos dados não estruturados dos servidores monitorados.

Além da visibilidade de permissões, usuários e grupos de segurança, deve ser possível gerar relatórios de permissionamento dos usuários e grupos de segurança às pastas e diretórios dos servidores monitorados através da interface gráfica da solução.

6.3. LOGS DE AUDITORIA MONITORADOS

A solução deve coletar de forma automática e continua logs de acessos a diretórios, pastas e arquivos dos servidores de arquivos monitorados, acessos a objetos do Active Directory (AD) e compartilhamento de arquivos.

Deve ser possível, na interface gráfica da solução, visualizar os logs de auditoria de acessos a diretórios, pastas e arquivos dos servidores monitorados, acessos a objetos do AD organizados e agrupados por recurso monitorado:

- Pasta ou diretório: demonstrar todos os eventos para aquela pasta, subpastas e arquivos;
- Unidade organizacional: demonstrar os eventos ocorridos em determinada OU;



- Usuário ou grupo de segurança: demonstrar os eventos gerados ou sofridos por determinado usuário ou grupo.

Os eventos de auditoria coletados pela solução devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.

As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários, grupos de segurança e dos servidores monitorados.

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

Todos os eventos dos diferentes servidores monitorados devem ser apresentados na mesma console gráfica da solução onde são também apresentadas as informações de permissionamento desses mesmos servidores monitorados.

A solução deve fornecer resumo das atividades auditadas, incluindo:

- Visualização dos usuários mais e menos ativos nos servidores monitorados;
- Visualização dos diretórios mais e menos acessados nos servidores monitorados;
- Visualização dos diretórios e pastas acessadas por um usuário ou grupo de segurança;
- Visualização dos usuários inativos em uma pasta ou diretório.



6.4. CARACTERÍSTICAS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO PARA AUDITORIA E OUTRAS FUNCIONALIDADES DE SERVIÇO DE DIRETÓRIO (MICROSOFT ACTIVE DIRECTORY).

As funcionalidades descritas nas características gerais devem se aplicar à solução para os serviços de diretórios de usuários do Microsoft Active Directory, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados.

A solução descrita neste item deve possuir as seguintes funcionalidades globais:

- Auditar ações sobre objetos do Active Directory;
- O software ofertado deve ter um compressor de dados para não onerar a banda;
- O software ofertado deve ser capaz de coletar os dados de forma nativa para a fonte de dados auditadas;
- Reter as informações de histórico em banco de dados por um período de acordo com a necessidade do solicitante;
- Ser capaz de rastrear as atividades dos usuários e administradores com informações detalhadas, incluindo quem, o que, quando, onde, qual estação de trabalho, para os eventos de alteração, além dos valores originais e atuais para todas as mudanças;
- Executar ações com base na auditoria, para contas de usuário ou computador de forma a permitir; desabilitar; remover; definir senha randômica; ou mover para OU específica, inclusive para múltiplas contas;
- Gerar alerta com base nas informações auditadas;
- Permitir aplicar password randômico em contas de usuário inativa;
- Monitorar e analisar comportamentos suspeitos de usuários;
- Identificar lacunas de Risk Assessment do ambiente para entender o impacto na segurança geral da TI com um painel com várias métricas sobre a avaliação de riscos de TI;
- Permitir agendamento de relatório;



- Permitir salvar ou exportar os relatórios nos formatos; Word, Excel, Powerpoint, PDF, TIFF, MHTML, CSV e XML;
- Permitir a filtragem dos relatórios de acordo com o objeto auditados;
- Permitir a criação de relatórios personalizado com informações inerentes do próprio ambiente;
- Permitir acesso para auditores poderem executar pesquisas e relatórios, sem fazer quaisquer alterações de configuração para a aplicação, sem necessidade de assistência e tempo dos administradores;
- Permitir o agendamento para envio de relatórios por e-mail e em uma determinada pasta do servidor sem a necessidade de customização adicional;
- O envio dos relatórios por e-mail deve ser feito a partir da própria solução, sem a utilização de software de terceiros e deve suportar o protocolo SMTP;
- Possibilitar relatórios customizáveis sob demanda e agendados;
- Ser capaz de fornecer relatórios para auditoria e conformidade (compliance);
- Deve suportar mecanismos de autenticação padrões de mercado como usuário/senha;
- O software ofertado deve ter API aberta para interação com outras ferramentas;
- O software ofertado deve ser capaz de fazer ajustes de auditoria no ambiente automaticamente;
- O software ofertado deve ser capaz de coletar os dados de forma nativa para a fonte de dados auditada.

6.5. FUNCIONALIDADE: AUDITAR AÇÕES SOBRE OBJETOS DO ACTIVE DIRECTORY

A solução deverá fornecer informações detalhadas de auditoria para perícia em relação aos seguintes pontos:

- Quem pode acessar e qual acesso pode fazer aos objetos do AD;



- Quem faz alteração nos objetos com a identificação do autor da criação, modificação e remoção de contas de usuário com data e hora dos eventos;
- Quem tem usado as credenciais para acessar os serviços de diretório;
- Detalhes dos eventos sobre objetos;
- Quem possui permissões sobre os objetos;
- Quem deu ou revogou permissões de acesso e modificação;
- Identificação de autor de criação, modificação e remoção de grupos com data e hora dos eventos;
- Possibilitar a identificação de conteúdo inserido e modificado;
- Permitir auditar a atividade de autenticação (autenticação interativa, interativa remota e logons de rede) incluindo logons com sucesso e falhos realizados nos servidores monitorados;
- Identificação de contas de usuário bloqueadas com data e hora dos eventos, incluindo endereços IP de origem e destino ou nome dos computadores de origem e destino;
- Identificação da última autenticação de conta de usuário no Active Directory com data, hora e origem (IP ou nome computador) dos eventos;
- Identificação de autenticações em computadores por conta de usuário com data e hora dos eventos, incluindo endereço IP ou nome computador;
- Identificação de autor de criação, modificação e remoção de contas de computadores com data e hora dos eventos;
- Possibilitar a identificação de conteúdo inserido e modificação.

A solução deverá ser capaz de rastrear quem fez alterações nos usuários, grupos, OUs e GPOs dos domínios monitorados do Active Directory, qual foi a alteração feita, quando foi feita, a máquina de origem da alteração e detalhes das propriedades tanto do objeto afetado quanto do objeto que gerou o evento.

A solução deverá indicar graficamente ou por relatório usuários ativos e inativos, usuários habilitados e desabilitados no AD.



A solução deve suportar a auditoria dos eventos do serviço de diretório, tais como:

- Criação e deleção de todos os objetos;
- Alteração de membros de grupos;
- Alteração nas propriedades dos objetos do serviço de diretório;
- Requisições de acesso;
- Autenticação de conta;
- Reconfiguração de senhas;
- Bloqueio e desbloqueio de conta;
- Criação e deleção de conta;
- Habilitação e desativação de conta;
- Eventos de permissão adicionada ou removida de objeto;
- Proprietário alterado;
- Identificação de autor de criação, modificação e remoção de objetos de diretivas de grupo com data e hora dos eventos;
- Possibilitar a identificação do conteúdo de configurações realizadas em objetos de diretivas de grupo;
- Identificação de autor de criação, modificação e remoção de unidades organizacionais com data e hora dos eventos;
- Possibilitar a identificação de conteúdo inserido e modificação.

A solução deve prover completa visibilidade sobre alterações em Objetos de Políticas de Grupos (GPO):

- Modificação de configuração de GPOs;
- Criação de link de GPO;
- Deleção de link de GPO;
- Modificação de link de GPO;
- Identificação de autor de criação, modificação e remoção de objetos de diretivas de grupo com data e hora dos eventos;



- Possibilitar a identificação do conteúdo de configurações realizadas em objetos de diretivas de grupo.

6.6. FUNCIONALIDADE: GERAR ALERTA COM BASE NAS INFORMAÇÕES AUDITADAS

A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado syslog, eventlog, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

- Atividades anômalas;
- Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos;
- Escalações de privilégios não autorizadas;
- Detecção de ferramentas de intrusão ou malwares.

O sistema de alerta em tempo real deve ser capaz de alarmar atividades em Active Directory (elevação de privilégios, inclusão/exclusão de grupos e usuários).

A solução deve permitir a integração com sistemas de e-mail padrão de mercado para envio de e-mails (alertas, notificações) de forma automática, ou manual.

6.7. FUNCIONALIDADE: RELATÓRIOS + INTEGRAÇÃO SIEM

6.7.1. A Solução deve permitir a integração com o SIEM

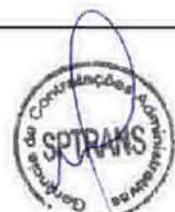
6.7.2. A Solução deve fornecer os seguintes relatórios:



- 6.7.2.1. Indicativos de uso de dados para a gestão de usuários, grupos de segurança e objetos do AD.
- 6.7.2.2. Logs de acessos e modificações de objetos do AD, com detalhamento dos eventos e metadados dos objetos afetados.
- 6.7.2.3. Usuários inativos no domínio.
- 6.7.2.4. Histórico de membros de grupos de segurança.
- 6.7.2.5. Estatísticas de autenticação e falha de autenticação.
- 6.7.2.6. Recomendações SCORE de revogação de permissões dos usuários calculadas pela análise comportamental.
- 6.7.2.7. Auditoria de todas as alterações do Active Directory por controlador de domínio.
- 6.7.2.8. Auditoria de todas as alterações do Active Directory por grupo.
- 6.7.2.9. Auditoria de todas as alterações do Active Directory por tipo de objeto.
- 6.7.2.10. Auditoria de todas as alterações do Active Directory por usuário.
- 6.7.2.11. Auditoria de todas as alterações do Active Directory com status de revisão.
- 6.7.2.12. Auditoria de alterações do contêiner de configuração do Active Directory.
- 6.7.2.13. Auditoria de alterações de contêiner de esquema do Active Directory.
- 6.7.2.14. Auditoria de alterações no site do Active Directory.
- 6.7.2.15. Auditoria de alterações na associação de grupos administrativos.
- 6.7.2.16. Auditoria de alterações na conta do computador.
- 6.7.2.17. Auditoria de alterações no objeto contato.
- 6.7.2.18. Auditoria de alterações no grupo de distribuição.
- 6.7.2.19. Auditoria de alterações no controlador de domínio.
- 6.7.2.20. Auditoria de alterações de confiança de domínio.
- 6.7.2.21. Auditoria de alterações na segurança dos objetos.
- 6.7.2.22. Auditoria de alterações na função de mestre de operações.
- 6.7.2.23. Auditoria de mudanças na Unidade Organizacional.



- 6.7.2.24. Auditoria de redefinições de senha pelo administrador.
- 6.7.2.25. Alterações em grupos de segurança dos domínios monitorados.
- 6.7.2.26. Grupos de segurança vazios ou não utilizados.
- 6.7.2.27. Usuários desabilitados que ainda fazem parte de grupos de segurança.
- 6.7.2.28. Lista de usuários administradores em grupos não administrativos.
- 6.7.2.29. Auditoria de instalações do Service Pack.
- 6.7.2.30. Auditoria de alterações na conta do usuário.
- 6.7.2.31. Auditoria de alterações no status da conta do usuário.
- 6.7.2.32. Auditoria de alterações de senha do usuário.
- 6.7.2.33. Auditoria de grupos.
- 6.7.2.34. Auditoria de membros do grupo.
- 6.7.2.35. Auditoria de participação efetiva no grupo.
- 6.7.2.36. Auditoria de membros do grupo administrativo.
- 6.7.2.37. Auditoria de contas de computador.
- 6.7.2.38. Auditoria de nomes principais de serviço das contas de computador.
- 6.7.2.39. Auditoria de usuários que não estão em nenhum grupo de distribuição.
- 6.7.2.40. Auditoria de controladores de domínio.
- 6.7.2.41. Auditoria de nomes principais de serviço dos controladores de domínio.
- 6.7.2.42. Auditoria de unidades Organizacionais.
- 6.7.2.43. Informações sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs dos domínios monitorados.
- 6.7.2.44. Auditoria de contas da unidade organizacional.
- 6.7.2.45. Auditoria de contas de usuário.
- 6.7.2.46. Auditoria de contas de usuário – expiradas.
- 6.7.2.47. Auditoria de contas de usuário – Bloqueadas.
- 6.7.2.48. Auditoria de contas de usuário - Senhas nunca expiram.
- 6.7.2.49. Auditoria de contas de usuário - Associação ao grupo.



- 6.7.2.50. Auditoria de contas de usuário - Último horário de logon.
- 6.7.2.51. Auditoria de todas as alterações de diretiva de grupo.
- 6.7.2.52. Auditoria de todas as alterações de diretiva de grupo por grupo.
- 6.7.2.53. Auditoria de todas as alterações de política de grupos com status de revisão.
- 6.7.2.54. Auditoria de alterações na política da conta.
- 6.7.2.55. Auditoria de renomeação de contas de administrador e convidado.
- 6.7.2.56. Auditoria de alterações no modelo administrativo.
- 6.7.2.57. Auditoria de alterações na política de auditoria.
- 6.7.2.58. Auditoria de alterações no link do GPO.
- 6.7.2.59. Auditoria de alterações interativas nas configurações de logon.
- 6.7.2.60. Auditoria de alterações na política de senha.
- 6.7.2.61. Auditoria de alterações nas políticas de chave pública.
- 6.7.2.62. Auditoria de alterações na política do registro.
- 6.7.2.63. Auditoria de alterações na política de grupos restritos.
- 6.7.2.64. Auditoria de alterações nas configurações de segurança.
- 6.7.2.65. Auditoria de alterações na política de restrição de software.
- 6.7.2.66. Auditoria de alterações nas configurações de software.
- 6.7.2.67. Auditoria de alterações na política de serviços do sistema.
- 6.7.2.68. Auditoria de alterações na configuração do usuário.
- 6.7.2.69. Auditoria de alterações na política de atribuição de direitos do usuário.
- 6.7.2.70. Auditoria de alterações nas configurações do Windows.
- 6.7.2.71. Auditoria de alterações na diretiva de rede sem fio.
- 6.7.2.72. Os relatórios devem possibilitar a exportação pelo menos no formato CSV, PDF, Excel, PowerPoint, Arquivo XML ou a possibilidade de imprimir em formato PDF.

6.8. CARACTERISTICAS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO PARA AUDITORIA E OUTRAS FUNCIONALIDADES DE SERVIDOR DE ARQUIVOS WINDOWS

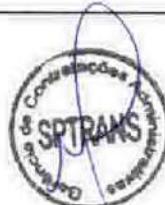
As funcionalidades descritas nas características gerais devem se aplicar para a solução de servidores de arquivos Windows.

A solução descrita neste item deve possuir as seguintes funcionalidades globais:

- Auditar acesso, criação, modificação e remoção de pastas e arquivos em servidores de arquivos com data e hora dos eventos;
- Possibilitar a identificação de conteúdo inserido e modificado;
- Executar ações proativas alertas com base na auditoria, inclusive para múltiplos objetos;
- Monitorar e analisar comportamentos suspeitos de usuários;
- Habilidade de fazer buscas, gerar relatórios e alertar mudanças ocorridas em um arquivo específico, pasta, pasta compartilhada ou todos os drives em um sistema de arquivos Windows;
- Ter capacidade de auditar arquivos, pastas de alterações indevidas;
- Gerar alerta com base nas informações auditadas e receber alertas em tempo real quando alguém tenta acessar algum arquivo ou pasta protegido de um servidor Windows;
- Deve suportar mecanismos de autenticação padrões de mercado como usuário/senha.

Rastrear todos os eventos relacionados a ações de pastas:

- Acesso a pasta falhou;
- Falha no acesso a pasta compartilhada;
- Mudança nas permissões da pasta;
- Mudança nos atributos da pasta;
- Mudança na auditoria da pasta;
- Mudança na política central de acesso da pasta (Windows Server 2012 R2 ou Windows Server 2016);



- Criação de pasta;
- Pasta apagada;
- Pasta Movida;
- Proprietário da pasta alterado;
- Pasta renomeada;

Rastrear todos eventos relacionados a ações de arquivos:

- Acesso ao arquivo falhou;
- Mudança de permissões do arquivo;
- Mudança de atributos do arquivo;
- Mudança de auditoria do arquivo;
- Arquivo criado;
- Arquivo apagado;
- Última alteração de arquivo;
- Arquivo movimentado;
- Mudança no proprietário (owner) do arquivo;
- Arquivo renomeado.

A solução deve suportar servidores virtuais de arquivos com a versão Windows Server 2012 ou superior.

A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios monitorados além monitorar os usuários que tem permissão de criação de pastas e permissões para que a gestão do repositório seja centralizada.

A solução deve fornecer relatório e de ajuste aos diretórios com herança quebrada de permissões.

O painel de controle (Dashboard) da solução deverá permitir a busca por um usuário ou grupo de segurança e deverá apresentar suas permissões nas caixas



postais e pastas dos servidores monitorados de forma integrada.

As informações apresentadas incluem:

- Identificação de herança de permissão ativada/desativada;
- Indicação de existência de compartilhamento;
- A fonte da permissão, ou seja, de que grupo o usuário está herdando a permissão

6.8.1. FUNCIONALIDADE: GERAR ALERTA COM BASE NAS INFORMAÇÕES AUDITADAS

A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado syslog, eventlog, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

- Atividades anômalas;
- Acesso a dados sensíveis;
- Arquivos sensíveis acessados ou excluídos;
- Escalações de privilégios não autorizadas;
- Modificação de permissões em diretórios sensíveis;
- Detecção de ferramentas de intrusão ou malwares.

A solução de alerta em tempo real deve ser capaz de alarmar atividades em arquivos (deleção, abertura, movimentação, acessos negados, entre outras).



6.8.2. FUNCIONALIDADE: MONITORAR E ANALISAR OS COMPORTAMENTOS SUSPEITOS DE USUÁRIOS

Baseada nos dados de auditoria, a solução deve ser capaz de apresentar o comportamento fora do padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.

A solução deve oferecer relatório dos alertas de comportamento anômalo identificados nos arquivos, pastas e diretórios dos servidores monitorados.

O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Office 365) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tais como:

- Quantidade e tamanho total dos arquivos e pastas;
- Dados sensíveis, parados e expostos;
- Pastas com permissões inconsistentes e usuários com ACEs diretas.

6.8.3. FUNCIONALIDADE: RELATÓRIOS

A Solução deve permitir a integração com o SIEM

A solução deve fornecer os seguintes relatórios:

- Indicativos de uso de dados para a gestão de arquivos e pastas;

- Logs de acessos e modificações de arquivos e pastas, com detalhamento dos eventos e metadados dos objetos afetados;
- Todas as modificações de permissionamento dos diretórios e pastas dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de arquivos;
- Pastas e diretórios dos servidores de arquivos monitorados onde há permissões concedidas a grupos de segurança globais (Everyone, Users ou Authenticated Users);
- Pasta ou de todas as pastas do servidor que possuem SIDs não resolvidos;
- Pasta ou de todas as pastas do servidor que tenham permissão direta aplicada a usuários;
- Dados inativos ou sem utilização no domínio;
- Histórico de permissões nas pastas e diretórios monitorados;
- Lista de pastas críticas com permissões excessivas nos servidores monitorados;
- Lista de permissões em pastas dos servidores monitorados de usuários desabilitados;
- Pastas dos servidores monitorados sem permissões de administradores;
- Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental;
- Estatística de acesso às pastas, utilização por tipo de arquivo, eventos por usuário e distribuição por tipos de evento sobre os servidores monitorados;
- Auditoria de todas as atividades do servidor de arquivos;
- Auditoria de todas as atividades do servidor de arquivos por tipo de ação;
- Auditoria de todas as atividades do servidor de arquivos por servidor;
- Auditoria de todas as atividades do servidor de arquivos por usuário;



- Auditoria de tentativas de alteração com falha;
- Auditoria de falha nas tentativas de exclusão;
- Auditoria de tentativas de leitura com falha;
- Auditoria de alterações no servidor de arquivos;
- Auditoria de alterações no servidor de arquivos por ação;
- Auditoria de alterações no servidor de arquivos por servidor;
- Auditoria de alterações no servidor de arquivos por usuário;
- Auditoria de arquivos e pastas criados;
- Auditoria de arquivos e pastas excluídos;
- Auditoria de arquivos e pastas movidos;
- Auditoria de arquivos e pastas renomeados;
- Auditoria de arquivos copiados;
- Auditoria de alterações de pasta;
- Auditoria de tipos de arquivo mais usados;
- Auditoria de compartilhar alterações;
- Auditoria de leituras bem-sucedidas de arquivos;
- Auditoria de resumo da atividade do usuário;
- Auditoria de permissões da conta;
- Auditoria de arquivos duplicados;
- Auditoria de pastas vazias;
- Auditoria de permissões de acesso excessivo;
- Auditoria de arquivos e pastas pelo proprietário;
- Auditoria de relatório de resumo da pasta;
- Auditoria de maiores arquivos;
- Auditoria de permissões de objeto por objeto;
- Auditoria de possíveis proprietários de dados por pasta;
- Auditoria de dados antigos por pasta;
- Auditoria de principais proprietários por tamanho total do arquivo.

Os relatórios devem possibilitar a exportação pelo menos no formato CSV, PDF, Excel, PowerPoint, Arquivo XML ou a possibilidade de imprimir em formato PDF.



7. SOLUÇÃO PARA VARREDURA DE VULNERABILIDADES

A solução proposta que será adotada pela proponente, deverá permitir a varredura de vulnerabilidades de todos os sistemas operacionais mencionados, equipamentos e demais dispositivos de diferentes fabricantes e não apresentar restrições, nem limitações quantitativas para varreduras conforme lista de referência de equipamentos e serviços no ambiente da SPTRANS.

A solução de varreduras adotada pela PROPONENTE, deverá ser capaz de analisar toda a infraestrutura de TI da SPTRANS conforme descritivos e quantitativos informados.

O serviço proposto para varredura de vulnerabilidades deverá ser capaz de analisar os diversos gerenciadores de banco de dados conforme quantitativos de referência informados, independente de fabricante, modelo ou versão, não sendo necessárias varreduras dos bancos de dados efetivamente.

As aplicações WEB no ambiente da SPTRANS, deverão ser analisadas para vulnerabilidades em seus serviços (por exemplo IIS, Apache, Tom Cat, Glassfish), infraestrutura onde a aplicação é executada.

A solução adotada pela CONTRATADA deverá ser capaz de verificar vulnerabilidades em gerenciadores de virtualização como Hyper-V e VMware;

A solução adotada deverá apresentar capacidade para análise de vulnerabilidades na estrutura do Active Directory (AD);

A solução definida deverá ser capaz de prover a autenticação através de autenticação via AD (Active Directory) ou LDAP;



A solução definida deverá ser escalável em quantidade de varreduras de vulnerabilidades possíveis, suportando eventual crescimento do parque computacional da CONTRATANTE sem que haja necessidade de mudança de ferramenta para suportar tal crescimento ou demanda;

Deve ter a capacidade de detecção de bug chain e vulnerabilidades de lógica e de regras de negócio, exemplo IDOR).

A solução deverá permitir desenvolvimento e adequação a necessidades particulares da SPTRANS, permitindo a inclusão de testes sobre as plataformas específicas.

7.1. CARACTERÍSTICAS TÉCNICAS PARA SOLUÇÃO VARREDURA DE VULNERABILIDADES

- 7.1.1. Todo o tráfego de informações entre a Solução e a Internet deve ser criptografado;
- 7.1.2. Todo o tráfego de informações entre o Gerenciador e os scanners deve ser criptografado.
- 7.1.3. Todos os scanners devem ser administrados por um Gerenciador único.
- 7.1.4. A solução deve possuir capacidade de receber atualizações em horários programados.
- 7.1.5. A solução deve suportar vários scanners conectados simultaneamente. Deverá a CONTRATADA utilizar quantos scanners sejam necessários para atender o sizing de itens de configuração especificados neste Termo de Referência, sem que haja necessidade de licenciamento adicional.
- 7.1.6. A solução deve possuir capacidade de atualizar os scanners automaticamente.
- 7.1.7. A solução deve receber a atualização automática da base de vulnerabilidades.



- 7.1.8. A solução deve possuir uma base de vulnerabilidades fornecida pelo fabricante, que deve ser atualizada de forma incremental diretamente do site do fabricante.
- 7.1.9. A solução deve possuir uma base de análises que permite identificar vulnerabilidades CVE.
- 7.1.10. A solução deve possuir em sua base de vulnerabilidades, para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, (CVE, CWE, BugTraq ou outra fonte), solução e link para o download da correção (se aplicável), contramedidas (se aplicável), informação e apresentação do exploit.
- 7.1.11. Se necessário, o scanner da solução deve funcionar sem necessidade de acesso à internet
- 7.1.12. A solução deve prover o registro de atividades (logs) para fins de auditoria, no mínimo para os eventos de: data e hora, endereço IP da origem da conexão, identificação do usuário e atividades executadas na ferramenta.
- 7.1.13. A solução deve prover interface gráfica WEB para gerenciamento de todos os seus componentes e suas configurações.
- 7.1.14. A solução deve possuir suporte ao IP (Internet Protocol) versão 4 e versão 6.

8. REQUISITOS TÉCNICOS DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES

Serão aceitas soluções em forma de "appliance", "virtual appliance" ou software para instalação em máquina virtual.

Deverá a solução estar disponível em sua última versão disponível e contar com suporte integral durante toda a vigência do contrato.

Deverá a solução adotada para prestação dos serviços de varredura de vulnerabilidades não constar no momento da apresentação da proposta, em listas



de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderá ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar no catálogo atualizado do fabricante.

Não poderá a solução estar em versão beta ou não contar com suporte do fabricante para versão definida.

Solução deverá permitir a descoberta dos ativos da rede (servidores, ativos de rede ou serviços que possuam endereço IP) sem a necessidade de agentes para esse fim.

A solução deverá ter capacidade de realizar automaticamente (através de agendamento automático) a descoberta de ativos;

A solução deve ter um console que permita um gerenciamento centralizado de relatórios e análises de vulnerabilidades dos servidores ou ativos de rede que possuam endereço IP ou que sejam alocados no escopo desta contratação.

Permitir detectar vulnerabilidades em servidores Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.

Permitir verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hotfixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus.

Supor tar efetuar varredura à procura de vulnerabilidades e exploits.

Integrar-se com base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures).

Possuir módulos de varredura diferenciados para análise mais intrusiva e não intrusiva.

Efetuar varredura por endereço IP, range de IP, agrupamento de ativos, nome NetBIOS ou CIDR Notation.

A solução deve possuir a capacidade de agendar varreduras de vulnerabilidades.

A solução deve ser capaz de executar varreduras de vulnerabilidades sob demanda.

A solução deve possibilitar a interrupção de uma varredura de vulnerabilidades, em qualquer momento da operação.

A solução deve ser capaz de emitir notificação por e-mail quando uma varredura de vulnerabilidades terminar.



Gerenciador deve possibilitar a configuração de desempenho na varredura de vulnerabilidades, como por número de conexões simultâneas e ativos simultâneos. A solução deve permitir a integração com as API's da Amazon e Microsoft Azure de serviços em cloud, a fim de descobrir imagens, ativas ou paradas, sem necessidade de escaneamento de rede.

Possuir capacidade de definir o número de alvos (IPs) para scanear simultaneamente e também a velocidade de forma a não impactar a desempenho da rede.

Deve permitir o cadastramento de credenciais utilizadas para escaneamento para que seja permitido o uso de tais credenciais para futuros escaneamentos, sem que o administrador da ferramenta saiba a senha destas credenciais.

A solução deve possibilitar a integração com pelo menos 1 (uma) solução de cofre de senhas para recuperação automática de credenciais no momento da execução do escaneamento.

A solução deve permitir a varredura de PII (Personable Identifiable Information) a fim de buscar informações sensíveis como, por exemplo, números de cartão de crédito em arquivos texto.

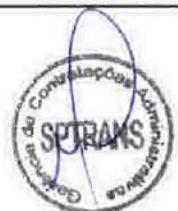
8.1.A FERRAMENTA DEVE PERMITIR ESCANEAMENTOS ESPECÍFICOS, UTILIZANDO NO MÍNIMO OS SEGUINTEIS GRUPOS DE AUDITORIA:

- 8.1.1. Deve possuir templates para varredura de vulnerabilidades mobile
- 8.1.2. Deve possuir templates para varredura de vulnerabilidades web application
- 8.1.3. Deve possuir templates para varredura de vulnerabilidades patch audit
- 8.1.4. Deve possuir templates para varredura de vulnerabilidades de acordo CIS
- 8.1.5. Deve possuir templates para varredura de vulnerabilidades de acordo PCI
- 8.1.6. Deve possuir condição de criação de modelos específicos com base no levantamento automatizada.



- 8.2. A solução de SIEM adotada deverá apontar os patches necessários, com possibilidade de correlacionar as informações pela própria interface da ferramenta de gerenciamento de vulnerabilidades.
- 8.3. Este mecanismo deve possibilitar a visualização de todos os patches disponíveis para um determinado host e permitir a visualização destes patches por tipo de patch, como críticos, atualizações de segurança, importantes, etc.
- 8.4. A solução deve possuir padrões de varredura de conformidade ou “benchmarking” pelo menos nos padrões: DISA Gold Disk, SCAP, NIST, FDCC, USGCB, CIS, Microsoft e etc.
- 8.5. A solução deve prover modelo de validação de conformidade para a Norma PCI DSS.
- 8.6. A solução deve ser capaz de criar internos tickets para tratamento de vulnerabilidades, e distribuir estes para os usuários da Solução.
- 8.7. A solução deve ser capaz de enviar e-mails para criação de tickets externos para tratamento de vulnerabilidades em ferramentas de ITSM externas.
- 8.8. A solução deve ser compatível pelo menos com os seguintes sistemas operacionais:
 - Windows Server 2008 SP2 ou maior (32-bits e 64-bits)
 - Windows 7 (32-bits e 64-bits)
 - Windows Server 2008 R2 SP1 ou maior (64-bits)
 - Windows 8 (32-bits e 64-bits)
 - Windows Server 2012 (64-bits)
 - Windows 8.1 (32-bits e 64-bits)
 - Windows 10 (32-bits e 64-bits)
 - Windows Server 2012 R2 (64-bits)
 - Windows Server 2016 (64-bits)
 - Linux
 - MacOS

9. SOLUÇÃO PARA AUTOMAÇÃO, GESTÃO, DESCOBERTA, IMPLEMENTAÇÃO E



INVENTÁRIO DE PATCHES EM AMBIENTE DE SERVIDORES E ESTAÇÕES DE TRABALHO CONTEMPLANDO SISTEMAS OPERACIONAIS MICROSOFT E LINUX.

9.1. A Solução deve possuir as seguintes características:

- Discovery de novos ativos, através de ranges de rede, para ambiente de estações de trabalho ou servidores;
- Patch Scan – Funcionalidade deve ser capaz de analisar o ativo e checar quais as atualizações estão pendentes. A solução deve permitir Consultas de dispositivos predefinidos, Consultas de dispositivos definidos pelo usuário, Grupos de dispositivos, Dispositivos específicos ou Todos os dispositivos;
- Patch Deploy – Funcionalidade capaz de instalar ou remover patches identificados como necessários para os ativos de acordo com as publicações de cada software instalado;
- Vulnerability Scan – Funcionalidade capaz de realizar a varredura continua dos ativos em buscas de vulnerabilidades potenciais;
- Distribuição de software ou pacotes – a solução deve ser capaz de realizar a Instalação de softwares ou scripts de forma silenciosa;
- Automação – a solução deve permitir a criação de tarefas intuitivas para execução remota nos dispositivos sem a necessidade da interação do usuário final.

9.2. A Solução deverá suportar os seguintes sistemas operacionais:

- Windows 8.1;
- Windows 10 ;
- Windows Server 2008 R2 (com ESU activation);
- Windows Server 2012 R2;
- Windows Server 2016;
- Windows Server 2019;
- CentOS ;
- Debian;



- Oracle Enterprise;
 - Red Hat Enterprise;
 - SUSE Enterprise;
 - Ubuntu.

9.3. Patch management

9.3.1. Gerenciamento avançado e automatizado de Patches Microsoft (sistema Operacional, Softwares Microsoft, Hotfix e Services Packs)

9.3.2. Gerenciamento avançado e automatizado de Patches de terceiros como:

- Adobe;
 - Amazon;
 - Apache;
 - Apple;
 - Canneverbe Limited;
 - Cisco Webex LLC;
 - Citrix;
 - Don Ho;
 - dotPDN LLC;
 - Dropbox;
 - DsNET Corporation;
 - Evernote Corporation;
 - FileZilla;
 - Foxit Corporation;
 - GlavSoft LLC;
 - GNOME Foundation;
 - Google;
 - Igor Pavlov;
 - Irfan Skiljan;
 - KeePass;
 - Malwarebytes;

- Microsoft Corporation;
- Mozilla;
- Opera;
- Oracle;
- Peter Pawlowski;
- RARLab;
- RealVNC;
- RingCentral;
- Simon Tatham;
- TechSmith;
- The Audacity Team;
- The Document Foundation;
- Ubuntu;
- uvnc bvba;
- Vendor;
- VideoLAN;
- VSRevoGroup;
- WinMerge;
- WinSCP;
- Wireshark;
- Zoom;
- Zoom Video Communications Inc. and RingCentral Inc.

9.3.3. Todos os patches acima especificados devem ser automaticamente adicionados ao cloud do cliente no mesmo dia da release do fabricante e automática sem a necessidade de o cliente adicionar patches manualmente

9.3.4. Permitir a criação de patches personalizados

9.3.5. Permitir alterar validadores e processo de instalação de cada patch bem como seus métodos de detecção

9.3.6. Categorizar todos os patches de acordo com o sistema CVSS, CVSS Severity e Severity do fabricante do patch.



9.3.7. Permitir janelas de manutenção e agendamentos para detecção e aplicação de patches.

9.3.8. Permitir varreduras para detecção de patches.

9.4. Permitir remoção de patches

9.5. Permitir instalar patches com base no inventário de hardware e software, inventário do próprio patch, de acordo com risco, sites, data de lançamento ou fabricante.

9.6. Utilizar modo per-to-per para instalação de patches com base na tecnologia de torrent, criando um torrent privado exclusivo para um deploy rápido e eficiente.

9.7. Possuir relatórios nos formatos (PDF, DOC e XLS) de patch conforme descrito abaixo:

Patches Detectados	Por CVE Por Tipo de Patch Por Dispositivo
Vulnerabilidades de Segurança detectadas por dispositivo	Relatório com filtros primários exibindo uma lista de vulnerabilidades de segurança detectadas para cada dispositivo
Vulnerabilidades de Segurança detectadas agrupadas por família	Relatório com o número de dispositivos que apresentaram vulnerabilidades de segurança para cada família.



Patches Historico de Instalação	Por Patch
	Por Site
	Por Dispositivo
Avaliação de risco de segurança	Estatísticas de risco por tipo de dispositivo, contagem de patches ausentes e um cronograma em um intervalo de datas específico)
Vulnerabilidades de Segurança detectadas agrupadas por família	Relatório com o número de dispositivos que apresentaram vulnerabilidades de segurança para cada família.
Top X Patches	Lista os X principais patches detectados de todos os dispositivos selecionados em seu filtro Primário e Secundário. (Onde X é um número definível pelo usuário)
Top X Vulnerable Dispositivos	Lista dispositivos com patches detectados em ordem decrescente

9.8. Software Deploy

- 9.8.1. Realizar deploy de scripts nos formatos .bat, .reg, .ps1, .vbs, .cmd.
- 9.8.2. Realizar Deploy de softwares com suporte a execução remota seja .exe, .msi, .com e etc.
- 9.8.3. Realizar remoção de softwares usando pacote uninstall ou scripts.
- 9.8.4. Utilizar modo per-to-per para instalação de software ou script com base na tecnologia de torrent, criando um torrent privado exclusivo para um deploy rápido e eficiente.

9.9. Inventário

- 9.9.1. Possuir inventário de hardware e software.
- 9.9.2. Permitir criar querys de inventário.
- 9.9.3. Permitir usar dados de inventário para personalizar a dashboard.
- 9.9.4. Permitir usar dados de inventário para agrupar ou segregar devices.
- 9.9.5. Criar uma timeline de softwares e patches encontrados ou instalados nos devices.
- 9.9.6. Possuir um comparativo de inventário entre datas diferentes.



- 9.9.7. Realizar tarefas de update do inventário on-demand ou agendado.
- 9.9.8. Permitir deletar e limpar a base de inventário.
- 9.9.9. As varreduras de inventário são realizadas todos os dias automaticamente, mas podem ser executadas manualmente a qualquer momento.
- 9.9.10. No Windows, as informações de hardware e software são coletadas via WMI e qualquer coisa instalada na Microsoft Store.
- 9.9.11. No Linux, o inventário é coletado usando o protocolo Secure Shell (SSH).
- 9.9.12. Inventory pode ser útil para habilitar a implantação dinâmica de software, como dispositivos que possuem um software antigo instalado ou precisam de antivirus.
- 9.9.13. Possuir relatórios nos formatos (PDF, DOC e XLS) de patch conforme descrito abaixo:

Dispositivos sem X software instalado	<p>Lista todos os dispositivos que não tem um software específico instalado</p> <p>Nota: Apenas uma única aplicação pode ser usada</p>
Armazenamento em disco restante	Todos os dispositivos que tem x% ou menos da porcentagem de armazenamento disponível no disco C
Resumo de SO por Site	Um resumo (e contagem) de todos os sistemas operacionais espalhados em todos os dispositivos, agrupados por nome de Site.
Catalogo de software	<p>Contagem de todas as instalações de software nos dispositivos selecionados</p> <p>Nota: Multiplos fabricantes podem ser selecionados para o mesmo relatório.</p>



9.10. Automação de tarefas

- 9.10.1. A solução deve possuir módulo para criação de regras de automação para implementação de pacthes com funcionalidades como disparar ações, incluindo informações de endpoint como estado de vulnerabilidade, localização de rede, instalações de software, processos em execução e outras variáveis.
- 9.10.2. Possuir interface para o usuário arrastar e soltar objetos criando sequência ações como patching, implantação de software, varreduras de segurança e script completo (powershell, c #, VB.
- 9.10.3. Permitir o agendamento de rotinas para manutenção, como patching, varreduras de segurança ou implantação de software, as tarefas poderão ser executadas em um horário especificado ou de forma recorrente. Sempre inteligentes, as tarefas consultam os dispositivos e visam aqueles que precisam de atenção. Usando agendamento de tarefas de manutenção para iniciar e parar em programações precisas, ou janelas de blackout para proteger os dispositivos sensíveis do seu ambiente as tarefas mantêm você atualizado enquanto a produtividade dos funcionários é preservada. Os resultados devem ser gerados em relatórios completos para comprovação de conformidade.
- 9.10.4. Permitir a criação de políticas de automação para serem executadas em um intervalo constante. As regras podem ser definidas de acordo com a necessidade de cada área de negócio.
- 9.10.5. Permitir a criação de uma política para monitorar o comportamento de acordo com cada cenário visando proteger os padrões de saúde e segurança estabelecidos. Exemplos de políticas são:



- Monitoramento de CPU, RAM e espaço em disco.
- Inicialização e remoção de software indesejado.
- Identificação e encerramento de processo malicioso.

9.10.6. A solução deve permitir a obtenção de informações instantâneas em tempo real.

9.10.7. Possuir arquitetura que obtenha o feedback imediatamente, em vez de esperar que os dispositivos enviem informações.

9.10.8. Acompanhar e registrar todas as atividades e resultados.

9.10.9. Permitir em tempo real identificar o software de inicialização em todos os dispositivos, monitorar a integridade do dispositivo ou rastrear e identificar um processo ou mudança de estado nos dispositivos.

10. DLP – DATA LOSS PREVENTION

10.1. O Serviço de DLP (Data Loss Prevention), ou prevenção de perda de dados é o controle via software de prevenção de perda de dados que detecta possíveis transmissões de dados confidenciais impedindo que os mesmos sejam salvos, enviados ou movidos para determinados locais (dispositivos de armazenamento como pendrives, HD externo, e-mail, armazenamento em nuvem etc.);

10.2. A Solução consiste em um conjunto de políticas de segurança e regras que podem ser aplicadas com a ajuda de softwares especializados para reforçar o bloqueio contra possíveis invasores. Após a implantação, a empresa terá visibilidade como monitoramento on-line, proteção reforçada de todos os arquivos, aplicações e dispositivos interligados à rede empresarial. Em casos de



vazamento de dados, informações sigilosas podem ser gerados o reports conforme as configurações requisitadas pelas empresas;

10.3. A solução de DLP deverá ser:

- 10.3.1. Endpoint DLP: são softwares instalados diretamente nas estações da rede, protegendo vazamentos via pendrive, HD externo, sites e programas de armazenamento e;
- 10.3.2. Network DLP: Monitora os pontos de saída de dados da rede interna, podendo ser controlado por software ou hardware.

10.4. CONSOLE DE GERENCIAMENTO

- 10.4.1. Deve ter administração centralizada por console único de gerenciamento;
- 10.4.2. As configurações de todos os módulos de detecção e criação de relatórios deverão ser realizadas através da mesma console;
- 10.4.3. O gerenciamento da solução deve ser baseado em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação;
- 10.4.4. Criptografia (HTTPS/TLS, versão 1.2 ou superior). Também será aceita a instalação de aplicação cliente (console de gerência) nas estações dos analistas responsáveis pela gestão da solução;
- 10.4.5. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, em um dos sistemas operacionais:

10.4.5.1. Microsoft Windows Server;



-
- 10.4.5.2. Red Hat Enterprise Linux.
 - 10.4.6. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado;
 - 10.4.7. Deve possuir integração com Active Directory, para autenticação de usuários da solução;
 - 10.4.8. Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação;
 - 10.4.9. Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;
 - 10.4.10. Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;
 - 10.4.11. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;
 - 10.4.12. Deve permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);
 - 10.4.13. Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;
 - 10.4.14. Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;



- 10.4.15. Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados;
- 10.4.16. Deve possuir logs detalhados de auditoria de alterações de políticas;
- 10.4.17. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;
- 10.4.18. Deve ter suporte a servidores com hardware x86 e sistema operacional Windows ou Linux, não requerendo a utilização de appliance;

10.5. IMPLEMENTAÇÃO E GERENCIAMENTO DO AGENTE

- 10.5.1. O agente deve ser suportado no mínimo nos Seguintes Sistemas Operacionais:
 - 10.5.1.1. Microsoft: Windows 7 SP1, Windows 8 ou 8.1, Windows 10 ou superior, Windows Server 2008 R2 e versões superiores; Apple: MAC OS X 10.15.0 e versões superiores.
 - 10.5.2. A gerência da solução deverá ser responsável pela Distribuição (Deploy), Instalação, Gerenciamento e Desinstalação do Agente nas estações bem como deverá executar inventário das máquinas nas quais estão com agentes instalados, esse inventário deverá coletar informações cruciais para o uso ideal do agente de DLP na estação do usuário;
- 10.6. Essa instalação poderá ser remota de forma silenciosa e sem a intervenção do usuário.



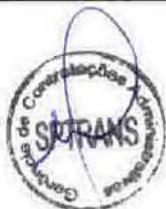
- 10.6.1. Um único agente deve executar todas as funções, inclusive a verificação de terminais e a monitoração e bloqueio de dados que saem do terminal.
- 10.6.2. Integra-se com os drivers do sistema operacional Windows em várias aplicações para garantir a estabilidade, interoperabilidade e segurança.
- 10.6.3. Atualizações dos agentes devem ser enviadas diretamente pela console de gerenciamento.
- 10.6.4. Segurança do Agente:
 - 10.6.4.1. As comunicações entre o agente e o servidor devem ser criptografadas e autenticadas;
 - 10.6.4.2. Deve permitir a opção de solicitação de senha para desinstalar o agente;
 - 10.6.4.3. Deve ter a capacidade de monitorar e bloquear tentativas de cópia de conteúdo confidencial para, no mínimo, os seguintes dispositivos (a ferramenta deve ser capaz de liberar a gravação ou somente leitura):
 - 10.6.4.3.1. Drives USB;
 - 10.6.4.3.2. CD/DVD;
 - 10.6.4.3.3. SD e Compact flash cards.
- 10.6.5. Deve ser integrável com ferramentas de criptografia, a fim de criptografar apenas o conteúdo confidencial enviado para um dispositivo USB ou e-mail;
- 10.6.6. Deve monitorar tentativas de cópia de conteúdo confidencial para o disco rígido e para compartilhamento na rede;



- 10.6.7. Deve exibir alerta "pop-up" na tela do usuário em caso de violação de política;
- 10.6.8. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial;
- 10.6.9. Deve permitir monitorar e bloquear transmissão FTP;
- 10.6.10. Deve, para um grupo pré-determinado de usuários, permitir o envio de informação confidencial, apresentando um "pop-up" de alerta quanto a criticidade da informação e solicitando confirmação da ação, a qual deve ser logada na console central;

10.7. CARACTERISTICAS GERAIS

- 10.7.1. A solução deverá utilizar banco de dados relacional SQL Server ou Oracle. Todas as licenças para uso do banco de dados devem ser fornecidas.
- 10.7.2. A solução deve permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
- 10.7.3. A solução deve ter capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
- 10.7.4. A solução deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.
- 10.7.5. A solução deve possuir módulos de detecção distintos, licenciados de forma independente, gerenciados por console único, para:



- 10.7.5.1. Localizar dados confidenciais armazenados em servidores de arquivos, intranet e bancos de dados;
- 10.7.5.2. Localizar dados confidenciais armazenados em desktops e laptops;
- 10.7.5.3. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP, capturando tráfego em modo promíscuo;
- 10.7.5.4. A solução deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações sensíveis detectadas;
- 10.7.5.5. A solução deve possuir, no mínimo, 60 modelos de políticas preexistentes produzidas, suportadas e atualizadas pelo fabricante da solução ou pelo CONTRATADO, que incluem palavras-chave e padrões de dados, para no mínimo, as principais normas internacionais HIPAA, Cobit, ISSO 27002, PCI, SOX e GDPR/LGPD;
- 10.7.6. Toda política criada na solução deve ser única, compatível e válida para aplicação em qualquer um dos módulos (agente, monitor de rede, scanner de dado armazenado).
- 10.7.7. A solução deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:
 - 10.7.7.1. Conteúdo detectado em arquivos e tráfego de rede (protocolos);
 - 10.7.7.2. Remetente e destinatário de correio;
 - 10.7.7.3. Tipo real (baseado em cabeçalho, não extensão), nome e tamanho do arquivo;
 - 10.7.7.4. Protocolo de comunicação utilizado;
- 10.7.8. A solução deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
 - 10.7.8.1. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR);



- 10.7.8.2. CAD (DWG, DXF, VSD, DGN);
- 10.7.8.3. Planilhas (XLS, XLSX, 123, SXC, ODS);
- 10.7.8.4. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
- 10.7.8.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);
- 10.7.8.6. Outros (PDF, MDB);
- 10.7.9. A solução deverá ter a capacidade de detectar e bloquear incidentes de tentativa de vazamento de informação confidencial, fornecendo detalhes dos arquivos oriundos dos incidentes na console da solução, com informações de contexto (hora, classificação, regras, propriedades, entre outros).
- 10.7.10. A solução deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo;
- 10.7.11. A solução deve possuir recursos avançados de inspeção de conteúdo, incluindo OCR.
- 10.7.12. A solução deve ter a capacidade de indexar através de impressão digital (hash) para dados estruturados e não estruturados;
- 10.7.13. A solução deve ter a capacidade de normalizar todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);
- 10.7.14. A solução deve possuir capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
- 10.7.15. Deve permitir a criação de dicionários de dados baseados em palavras-chave, frases e expressões regulares para serem usados nas regras de DLP;



- 10.7.16. A solução deve ter a capacidade nativa de detectar uma grande variedade de padrões de dados que representam dados confidenciais (por exemplo, CPFs, depósitos, dados da tarja magnética, IBAN);
- 10.7.17. A solução deve ter a capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, EUA, União Europeia, e Brasil;
- 10.7.18. A solução deve permitir detectar faixas de números válidos para determinados tipos de dados, tal como, no mínimo, número de cartão de crédito válido;
- 10.7.19. A solução deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails;
- 10.7.20. A solução deve ter a capacidade de bloquear a captura de tela (print screen) integral, ou seja, mesmo que seja de uma janela NÃO ativa no momento da captura;
- 10.7.21. A solução deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem;
- 10.7.22. A solução deve suportar a verificação de arquivos compactados recursivos (exemplo zip dentro de zip);
- 10.7.23. A solução deve identificar conteúdo armazenado em colunas específicas de planilhas eletrônicas e em bancos de dados;
- 10.7.24. A solução deve ser capaz de gerar incidentes para detecção se parte do conteúdo for copiado;



- 10.7.25. A solução deve, em um determinado incidente, permitir a verificação por assunto, remetente, destinatário, nome de arquivo, proprietário do arquivo, nome de usuário e política.
- 10.7.26. A solução deve exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.
- 10.7.27. A solução deve permitir ocultar certos dados, como informações de identidade do remetente, durante a visualização do Incidente na tela do Console, dependendo do nível de acesso dado ao operador da ferramenta, para no mínimo, os seguintes tópicos:
- 10.7.27.1. Endereço de e-mail;
 - 10.7.27.2. Nome de usuário;
 - 10.7.27.3. Proprietário do arquivo;
- 10.7.28. A solução deve permitir destacar na tela do incidente os dados confidenciais detectados;
- 10.7.29. A solução deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo;
- 10.7.30. A solução deve possuir mecanismo de envio de notificações personalizáveis através de e-mail, como casos de violação de política;
- 10.7.31. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações;
- 10.7.32. A solução deve ser permitir notificar automaticamente o remetente e o gerente ou superior hierárquico do usuário envolvido no incidente;



10.7.33. A solução deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

- 10.7.33.1. Bloqueio de mensagem;
- 10.7.33.2. Quarentena de arquivo;
- 10.7.33.3. Notificação ao usuário;
- 10.7.33.4. Bloqueio do acesso web, bloqueio de cópia e impressão;

10.7.34. A solução deve permitir armazenar a mensagem e o arquivo original que gerou o incidente;

10.7.35. A solução deve verificar existência de conteúdo confidencial em file systems para no mínimo CIFS, NFS, SMB e NTFS;

10.7.36. A solução deve permitir a análise dos file systems sem a necessidade de agentes nos servidores de origem;

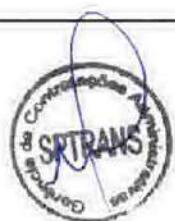
10.7.37. A solução deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP.

10.8. RELATÓRIOS

10.8.1. A solução deve permitir a emissão de relatório de incidentes e tendências por unidades e usuários, utilizando o LDAP (MS Active Directory) corporativo. A solução deve permitir agrupar, filtrar e classificar relatórios.

10.8.2. A solução deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:

- 10.8.2.1. Timestamp;
- 10.8.2.2. Tamanho e data do arquivo;



- 10.8.2.3. Endereço IP de origem e destino;
 - 10.8.2.4. Histórico de incidentes e detalhes;
 - 10.8.2.5. Remetente e destinatário.
- 10.8.3. A solução deve permitir exportar relatórios para formato PDF, HTML, XML ou CSV;
- 10.8.4. A solução deve ter capacidade de enviar relatórios por e-mail via agendamento (datas específicas e periodicamente);
- 10.8.5. A solução deve apresentar um painel de controle para visualização dos relatórios;
- 10.8.6. A solução deve ter a capacidade para configurar, salvar relatórios e painéis de controle personalizados por usuário;
- 10.8.7. A solução deve ter opção de publicar relatórios salvos para todos os usuários ou mantê-los como relatórios pessoais;
- 10.8.8. A solução deve permitir gerar relatórios resumidos por níveis, agrupados, summarizados e com capacidade de detalhamento.

11. DCS – DATA SECURITY EXTENDED

- 11.1. Data Center Security é uma solução baseada no fortalecimento de Segurança e Monitoramento para nuvem privada e Data Center Físicos;
- 11.2. Funcionalidade de Proteção aos sistemas operacionais atuais e descontinuados (exemplo Windows Server 2003) e outras plataformas legadas;



- 11.3. Deverá ter a capacidade de detectar e responder a ações de risco ao ambiente, permitindo ampliar a capacidade de resposta sem onerar o ambiente protegido e responder no menor tempo possível a ameaça;
- 11.4. O serviço deverá fornecer console centralizada (única) para visibilidade do ambiente protegido de estações de trabalho e servidores, onde deverão ser exibidas todas as informações necessárias para gerenciamento, auditoria e desempenho a contratante;
- 11.5. Todo o acesso a console e tráfego de dados deverá ser feito através de protocolo criptografado (HTTPS), utilizar túnel de segurança TLS, e funcionar em ao menos um dos principais navegadores de web (Google Chrome, Microsoft Edge e Firefox);
 - 11.5.1.
- 11.6. Toda a plataforma de administração do serviço é de responsabilidade da contratada, devendo essa garantir os níveis de segurança de acesso e armazenamento das informações, contendo no mínimo:
 - 11.6.1. Uso de segundo fator de autenticação;
 - 11.6.2. Autenticação baseada em relação de confiança com o domínio do contratante, com suporte a SSO (Single Sign On), sendo compatível, no mínimo, com Microsoft ADFS – Active Directory Federation Services.
- 11.7. Garantir permissões de acesso baseado em definições de papéis (RBAC) dos usuários do serviço;
- 11.8. A contratada deverá garantir o armazenamento dos dados em ambiente próprio ou ser autorizada a representar provedor de serviços que mantenha controle de segurança, disponibilidade, integridade e confidencialidade das informações;



11.9. Os dados coletados não devem ultrapassar a classificação de telemetria computacional, ou seja, deverão ser restritos a análise em tempo real de execução de sistemas operacionais e aplicações. É vedado a transmissão dados do ambiente da contratante, incluindo documentos em qualquer formato, base de dados, arquivos ou mídias sem o consentimento prévio do Contratante;

11.10. As informações de telemetria dos incidentes e ações ocorridas nos dispositivos protegidos deverão estar disponíveis na console centralizada independentemente do status dispositivo naquele momento (ligado ou desligado), ou seja, caso o dispositivo esteja inoperante, a investigação dos incidentes e eventos deverá ser possível;

11.11. Os dados de telemetria computacional analisadas pelo serviço devem incluir no mínimo as seguintes atividades:

- 11.11.1. Endereços de rede;
- 11.11.2. Login de usuários;
- 11.11.3. Informações de sistema operacional, modelo e última atividade;
- 11.11.4. Número de executáveis únicos;
- 11.11.5. Processos que foram executados;
- 11.11.6. Utilização de ferramentas administrativas;
- 11.11.7. Requisições DNS;
- 11.11.8. Conexões de rede incluindo portas e processos associados;
- 11.11.9. Scripts escritos em disco;
- 11.11.10. Mapa de geolocalização de conexões de rede.
- 11.11.11. Visibilidade sobre parâmetros de execução de um processo.

11.12. O serviço deverá trabalhar com indicadores de comprometimento (IOC's) e indicadores de ataques (IOA's);

11.13. A análise das informações é de responsabilidade da contratada, não devendo essa onerar a contratante com a estruturas computacionais, seja no



uso de equipamentos, como servidores de rede, ou com outros recursos como espaço em data center, refrigeração de equipamentos, eletricidade e qualquer outro componente que possa introduzir custos indiretos a contratante;

- 11.14. Para coleta da telemetria computacional a ser analisada a contratada poderá fazer uso de sensor (agente) a ser instalados por dispositivo protegido pelo Serviço que deverá operar em tempo real;
- 11.15. O sensor deverá ser único para cada dispositivo protegido, não devendo ser intrusivo a ponto de provocar impacto desempenho do dispositivo. Obedecendo as seguintes características:
 - 11.15.1. Ser instalado ou removido de forma silenciosa, não sendo necessário reiniciar o dispositivo monitorado, de maneira imperceptível para os usuários da rede corporativa da contratante e ininterrupto aos serviços digitais prestados;
 - 11.15.2. Consumir menos de 3% de processamento, utilizar menos de 100 Megabytes de memória RAM e não ocupar mais de 70 Megabytes de espaço em disco do dispositivo protegido.
- 11.16. Não será permitida a varredura de disco pelo sensor para análise de dados e arquivos nele contidos, onerando assim os dispositivos da contratante;
- 11.17. Os sensores do serviço não poderão ser desinstalados por usuário que não possua perfil administrativo no dispositivo monitorado, ou mesmo ter suas configurações alteradas sem tal requisito;
- 11.18. A desinstalação dos sensores do serviço deverá exigir senha ou utilizar de token para sua execução;
- 11.19. A senha deverá ser revelada na console centralizada do Serviço caso necessário;



- 11.20. O serviço deve proteger o ambiente corporativo obrigatoriamente das seguintes ameaças:
 - 11.20.1. Detectar Adware's e programas potencialmente indesejados;
 - 11.20.2. Ter capacidade de bloquear assinaturas digitais de arquivos (hashes);
 - 11.20.3. Conseguir bloquear scripts e comandos de Windows Powershell;
 - 11.20.4. Ser capaz de bloquear processos em execução em sistemas operacionais Microsoft Windows;
 - 11.20.5. Bloquear operações de registro no Microsoft Windows;
 - 11.20.6. Analisar e bloquear ações de ameaças já reconhecidas por soluções antimalware ou base de conhecimento específica;
- 11.21. Deve permitir a remoção para quarentena de arquivos comprovadamente maliciosos para futura investigação;
- 11.22. Deve utilizar de ASLR para mitigar a exploração de memória dos dispositivos protegidos;
- 11.23. Deve impedir ataques que utilizem região de espaço de memória não executável;
- 11.24. Proteger contra ataques Heap Spray Preallocation;
- 11.25. Proteger contra ataques baseados em SHE (Structured Exception Handling);
- 11.26. Impedir a exploração de vulnerabilidades causadas por ponteiros nulos;



- 11.27. Analisar comportamento de ataques do tipo Ransomware, impedindo ações de exclusão de backups, operações incomuns ou abusivas relacionadas a sistemas de arquivos e criptografia de arquivos;
- 11.28. Detectar comportamentos suspeitos originados de processos a partir de navegadores web;
- 11.29. Detectar o comprometimento de servidores via webshell;
- 11.30. Analisar a injeção de código entre processos;
- 11.31. Detectar anomalias no processo de login dos dispositivos protegidos que utilizem sistema operacional Microsoft Windows evitando a movimentação lateral não autorizada;
- 11.32. Analisar processos que tentem obter credenciais de login;
- 11.33. O serviço deve atender as seguintes técnicas e sub- técnicas do Mitre Att&ck:

T1003, T1003.001, T1003.002, T1012, T1018, T1021, T1021.001, T1021.002, T1021.004, T1021.006, T1026, T1027, T1027.002, T1027.003, T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1047, T1048, T1048.003, T1049, T1053, T1053.005, T1055, T1055.012, T1059, T1059.001, T1059.003, T1059.005, T1059.007, T1061, T1069.001, T1070, T1070.004, T1070.005, T1070.006, T1071.004, T1074.002, T1078.003, T1087, T1087.001, T1087.002, T1095, T1102, T1110, T1110.003, T1112, T1114.001, T1132, T1132.001, T1134.002, T1136, T1136.001, T1204, T1204.002, T1218, T1218.005, T1218.011, T1219, T1222, T1222.001, T1543, T1543.003, T1546.003, T1546.008, T1546.015, T1547, T1547.001, T1548, T1548.002, T1550, T1550.002, T1550.003, T1552.001, T1559, T1559.001, T1560, T1560.001, T1562, T1562.004, T1564, T1564.004, T1567, T1567.002, T1570, T1574, T1574.001.

- 11.34. Suportar no mínimo as RFC's 5246, 4346 e 8446;



11.35. O serviço deve ser capaz de executar ações manuais de remediação, realizada por operador ou administrador, de forma remota sem a ativação de softwares de terceiros no dispositivo protegido;

11.36. As ações remotas de remediação devem incluir:

- 11.36.1. Extração de arquivos;
- 11.36.2. Envio de arquivo para área de armazenamento externa ao dispositivo;
- 11.36.3. Execução de processos;
- 11.36.4. Dump de memória;
- 11.36.5. Execução de scripts automatizados remotamente.

11.37. As ações manuais de remediação devem ser interrompidas e seu recurso de acesso desativado caso assim determine o contratante;

11.38. O serviço deve ser capaz de gerenciar o acesso do dispositivo protegido na rede de maneira que bloquee, em caso de ataque ou atividade suspeita, a sua comunicação com outros dispositivos na rede de forma global ou granular, permitindo acesso a endereços específicos, evitando assim movimentações laterais indesejadas;

11.39. Mesmo bloqueado, o dispositivo deve responder a ações remotas de remediação;

11.40. A console centralizada de gestão do Serviço deverá obedecer às capacidades abaixo listadas e exibir as seguintes informações mínimas para servidores:

- 11.40.1. Prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.



- 11.40.2. Capacidade de reportar as detecções de forma agrupada tendo como opções de agrupamento no mínimo os seguintes critérios: Máquina, tática, técnica, severidade;
- 11.40.3. Capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.
- 11.40.4. Capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros: severidade, tática, técnica, usuário, host, tipo de sistema operacional, versão do sistema operacional, última hora, último dia, última semana, últimos 30 dias, nome de arquivo e hash do processo;
- 11.40.5. Capacidade de relatório de todas as conexões remotas realizadas desde a console de gerenciamento centralizada do Serviço ao dispositivo protegido contendo minimamente as seguintes informações que não deverão ser passíveis de exclusão ou limpeza, garantindo assim o não-repúdio:
 - 11.40.5.1. Login do administrador/operador que realizou a operação;
 - 11.40.5.2. Nome do endpoint;
 - 11.40.5.3. Duração da sessão;
 - 11.40.5.4. Data e hora do inicio da sessão;
 - 11.40.5.5. Arquivos copiados desde a máquina;
 - 11.40.5.6. Comandos executados na máquina;
 - 11.40.5.7. Caminho completo do arquivo copiado da máquina;
 - 11.40.5.8. Data e hora de cada comando executado;
- 11.40.6. Gerar relatório dos dispositivos protegidos contendo minimamente as seguintes informações, podendo ser exportada em CSV:
 - 11.40.6.1. Hostname;
 - 11.40.6.2. Data e hora da primeira comunicação;
 - 11.40.6.3. Data e hora da última comunicação;
 - 11.40.6.4. Versão do sistema operacional;



- 11.40.6.5. Modelo;
- 11.40.6.6. Tipo;
- 11.40.6.7. Unidade organizacional (OU);
- 11.40.6.8. Site;
- 11.40.6.9. Política de proteção aplicada;
- 11.40.6.10. Política de resposta aplicada;
- 11.40.6.11. Política de atualização aplicada;
- 11.40.6.12. Política de controle de dispositivos USB aplicada;
- 11.40.6.13. Política de firewall aplicada;
- 11.40.6.14. Identificação do host (UID/GUID);
- 11.40.6.15. IP local da máquina;
- 11.40.6.16. IP público da máquina;
- 11.40.6.17. MAC Address;
- 11.40.6.18. Versão do sensor instalado.

11.40.7. O relatório dos dispositivos protegidos deverá ter a capacidade de aplicar filtros para inclusão ou exclusão de dados no relatório, considerando minimamente as seguintes opções de filtro:

- 11.40.7.1. Domínio;
- 11.40.7.2. Grupo;
- 11.40.7.3. Identificação do host (UID/GUID);
- 11.40.7.4. Hostname;
- 11.40.7.5. IP local da máquina;
- 11.40.7.6. MAC Address;
- 11.40.7.7. Subnet da máquina;
- 11.40.7.8. Versão do sistema operacional;
- 11.40.7.9. Unidade organizacional (OU);
- 11.40.7.10. Plataforma;
- 11.40.7.11. Política de proteção aplicada;
- 11.40.7.12. Política de resposta aplicada;



- 11.40.7.13. Política de atualização aplicada;
- 11.40.7.14. Versão do sensor instalado.
- 11.40.8. Deverá possuir painel de controle (dashboard) contendo minimamente as seguintes informações:
- 11.40.8.1. Total de hosts vistos nas últimas 24 horas;
- 11.40.8.2. Total de estações vistos nas últimas 24 horas;
- 11.40.8.3. Total de servidores vistos nas últimas 24 horas;
- 11.40.8.4. Hosts comunicando na última hora;
- 11.40.8.5. Hosts off-line;
- 11.40.8.6. Hosts isolados/quarentenados;
- 11.40.8.7. Hosts com sensor sem proteção para desinstalação;
- 11.40.8.8. Total de dispositivos protegidos em cada política de proteção;
- 11.40.8.9. Total de dispositivos protegidos em cada política de resposta;
- 11.40.8.10. Total de dispositivos protegidos em cada política de atualização do sensor;
- 11.40.8.11. Total de dispositivos protegidos em cada política de controle USB.
- 11.41. Deve permitir a criação de fluxo de trabalho (Workflow) para automatização de processos, os quais devem incluir os seguintes recursos:
- 11.41.1. Verificação da cadeia de execução do Workflow;
- 11.41.1.1. Compreender gatilhos de execução baseados em:
- 11.41.1.1.1. Novos Incidentes;
- 11.41.1.1.2. Novas detecções;
- 11.41.1.1.3. Eventos de auditoria, incluindo os parâmetros: atribuição, status, comentários e políticas.



11.42. Permitir ações diretas no dispositivo, como:

- 11.42.1. Baixar um arquivo;
- 11.42.2. Remover um arquivo;
- 11.42.3. Executar pesquisas no VirusTotal;
- 11.42.4. Conter comunicação do dispositivo na rede;
- 11.42.5. Atualizar informações de uma detecção ou incidente, permitindo adicionar comentários, assinar a um usuário do sistema, mudar o status.

11.43. CARACTERÍSTICAS ESPECÍFICAS PARA O SERVIÇO DE VISIBILIDADE E PROTEÇÃO DE ESTAÇÕES DE TRABALHO

11.43.1. As informações de telemetria dos incidentes e ações ocorridas nos dispositivos protegidos deverão estar disponíveis na console centralizada independentemente do status dispositivo.

11.43.2. O Serviço deverá garantir a visibilidade e proteção de dispositivos que utilizem, no mínimo, os seguintes sistemas operacionais:

11.43.3. Microsoft Windows 8.1 ou superior;

11.43.4. MacOS 10.15 ou posterior.

11.43.5. O serviço deve implementar gestão no uso da interface USB dos dispositivos, controlando as seguintes classes de componentes USB:

11.43.5.1. Dispositivos de armazenamento de imagens, vídeos e áudios;

11.43.5.2. Dispositivos de armazenamento de arquivos (flash disk e pendrives)

11.43.5.3. Dispositivos móveis (MTP/PTP)

11.43.5.4. Impressoras

11.43.5.5. Adaptadores de redes wifi;

- 11.43.6. O controle de componentes USB deve incluir ações do tipo: bloqueio, escrita, execução e leitura;
- 11.43.7. O controle de componentes USB deve permitir a criação de regras de acesso baseadas em Vendor ID e Product ID, número de série e classe;
- 11.43.8. O Serviço deve ser capaz de implantar a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no dispositivo protegido;
- 11.43.9. As regras de firewall devem ser agrupáveis;
- 11.43.10. Regras de firewall devem suportar minimamente as seguintes características:
 - 11.43.10.1. IPv4 e IPv6;
 - 11.43.10.2. Protocolos Any, TCP, UDP, ICMP;
 - 11.43.10.3. Endereço local;
 - 11.43.10.4. Porta local;
 - 11.43.10.5. Endereço remoto;
 - 11.43.10.6. Porta remota de conexão;
 - 11.43.10.7. Ação de permitir e bloquear;
 - 11.43.10.8. Direção da conexão Inbound ou Outbound;
 - 11.43.10.9. Perfil de rede: Domínio privado, público;
 - 11.43.10.10. Processo.
- 11.43.11. Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;
- 11.43.12. As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente;
- 11.43.13. O Serviço deve exibir, no mínimo, as seguintes visualizações na console:
 - 11.43.13.1. Sensores ativos;
 - 11.43.13.2. Sensores por sistema operacional;



- 11.43.13.3. Detecções por objetivo do ataque ao dispositivo protegido;
- 11.43.13.4. Detecções por tática do ataque ao dispositivo protegido;
- 11.43.13.5. Detecções por severidade do ataque ao dispositivo protegido.

11.44. CARACTERÍSTICAS ESPECÍFICAS PARA O SERVIÇO DE VISIBILIDADE E PROTEÇÃO DE SERVIDORES

11.44.1. O Serviço deverá garantir o armazenamento da telemetria, independentemente se essa foi ou não classificada como uma ameaça, por no mínimo 7 dias e possibilitar a análise da contratante nesse período na console centralizada;

11.44.2. O Serviço deverá apontar na console alerta de indícios de atividades maliciosas baseado na análise da telemetria e comportamento. Esse alerta deverá ser validado por especialista da plataforma e não apenas por tecnologia de "machine learning" e/ou "behavior analytics";

11.44.3. O Serviço deve possuir ferramenta de busca por informações coletadas através de sintaxes que filtrem a busca sem a necessidade de que o(s) dispositivo(s) esteja(m) disponível, concatenando critérios:

- 11.44.3.1. Deve permitir a busca por hashes MD5 e SHA256;
- 11.44.3.2. Deve permitir buscas por nomes de arquivo;
- 11.44.3.3. Deve permitir a busca por atividades de usuário;
- 11.44.3.4. Deve permitir extração de dados em formato CSV e JSON.

11.44.4. O Serviço deverá garantir a visibilidade e proteção de dispositivos que utilizem, no mínimo, os seguintes sistemas operacionais:

- 11.44.4.1. Microsoft Windows Server 2012 ou superior;
- 11.44.4.2. Linux CentOS 8.0;
- 11.44.4.3. Linux Red Hat Enterprise (RHEL) 8.0;



- 11.44.4.4. Linux Suse Enterprise 15;
- 11.44.4.5. Ubuntu 18.

11.44.5. O Serviço deve exibir, no mínimo, as seguintes visualizações na console:

- 11.44.5.1. Sensores ativos;
- 11.44.5.2. Sensores por sistema operacional;
- 11.44.5.3. Detecções por objetivo do ataque ao dispositivo protegido;
- 11.44.5.4. Detecções por tática do ataque ao dispositivo protegido;
- 11.44.5.5. Detecções por severidade do ataque ao dispositivo protegido;
- 11.44.5.6. Top 10 de detecções por dispositivo protegido;
- 11.44.5.7. Top 10 de detecções por usuário;
- 11.44.5.8. Top 10 de detecções por arquivos;
- 11.44.5.9. Sensores ativos por localização geográfica.

12. TESTE DE INTRUSÃO/PENETRAÇÃO

12.1. As atividades de Teste de Intrusão/Penetração (Pentest) devem compreender:

12.1.1. Realização de teste de penetração digital semi-orientado "Grey-box penetration test" com equipe de ataques ofensivos "red team" realizando testes manuais e ferramentas automatizadas no site e na infraestrutura que o suporta (sistemas operacionais, servidores web, servidores de aplicação, servidores de banco de dados, entre outros), para elaboração de relatórios e posterior direcionamento da correção das fragilidades detectadas;

12.1.2. Realização de teste de penetração digital cego "Black-box penetration test" com equipe de ataques ofensivos "red team" realizando



testes manuais e ferramentas automatizadas no site e na infraestrutura que o suporta (sistemas operacionais, servidores web, servidores de aplicação, servidores de banco de dados, entre outros), para elaboração de relatórios e posterior correção das fragilidades detectadas;

12.1.3. Testes de Invasão Externos e Internos e tem como objetivo principal identificar, possíveis vulnerabilidades na infraestrutura tecnológica da CONTRATANTE.

12.2. O Teste de Negação de Serviço (DDoS) deve compreender a verificação da quantidade e do tipo de tráfego suportado pela infraestrutura do CONTRATANTE, apresentar os riscos e as soluções para minimizar o impacto de um ataque de indisponibilidade real.

12.3. Teste de Penetração Interno.

12.3.1. A CONTRATADA deverá realizar 1 teste intrusão por mês (limitando-se à 12 testes de intrusão por ano) para identificação de vulnerabilidades por meio de simulações de invasão de aplicações e infraestrutura (Teste de Invasão) a serem executadas internamente (através da rede interna da CONTRATANTE).

12.4. Teste de Penetração Externo.

12.4.1. A CONTRATADA deverá realizar de forma recorrente automatizada e manual para identificação de vulnerabilidades por meio de simulações de invasão de aplicações e infraestrutura, as ações manuais deverão ter testes diários pela equipe contratada a fim de mitigar ao máximo as principais aplicações e sistemas críticos.

12.5. Todas as vulnerabilidades encontradas no pentest manual deverão ser entregues em um relatório com medidas de correções assim como o exploit utilizado ou prova de conceito para reproduzir a falha.



- 12.6. A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências apuradas; fontes de pesquisa, referências e ferramentas utilizadas.
- 12.7. A CONTRATADA deverá elaborar o "Plano de Teste de Invasão", para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; equipe envolvida; prazos do teste.
- 12.8. Deverão ser testados, minimamente, os seguintes quesitos, quando pertinentes:
- 12.8.1. Validação de acesso lógico
 - 12.8.2. Segmentos de rede
 - 12.8.3. VLANs
 - 12.8.4. Burlar regras de firewall
 - 12.8.5. Obtenção de informações
 - 12.8.6. Enumeração de usuários
 - 12.8.7. Sniffing
 - 12.8.8. ARP Spoofing
 - 12.8.9. Segurança dos dados
 - 12.8.10. Canal de comunicação
 - 12.8.11. Cifras fracas
 - 12.8.12. Armazenamento inseguro
 - 12.8.13. Descoberta de Senhas
 - 12.8.14. Força bruta



- 12.8.15. Ataque off-line
- 12.8.16. Arquitetura da rede
- 12.8.17. Acesso remoto e VPN
- 12.8.18. Protocolos de comunicação
- 12.8.19. Mixed Content/Scripting;
- 12.8.20. Unvalidated Redirects;
- 12.8.21. Insecure Cookies;
- 12.8.22. Iframe Injection;
- 12.8.23. Clickjacking;
- 12.8.24. Cross Site Scripting (XSS);
- 12.8.25. Cross Site Request Forgery (XSRF);
- 12.8.26. Cross Site Script Inclusion (XSSI);
- 12.8.27. HTTP Parameter Pollution;
- 12.8.28. Path Traversal;
- 12.8.29. Buffer Overflow;
- 12.8.30. Integer Overflow;
- 12.8.31. Privilege Escalation;
- 12.8.32. Authentication Bypass;
- 12.8.33. Information Leak;
- 12.8.34. Local File Inclusion;
- 12.8.35. Remote File Inclusion;
- 12.8.36. Source Code Disclosure;
- 12.8.37. SQL Injection;
- 12.8.38. Remote Code Execution;
- 12.8.39. Revisão das vulnerabilidades listadas no OWASP Top 10
- 12.8.40. Insecure Direct Object Reference.

12.9. A CONTRATADA deverá elaborar um relatório de auditoria com os testes realizados, vulnerabilidades encontradas e recomendações de melhoria. O relatório técnico deve ser detalhado e deve ser acompanhado de uma apresentação executiva sobre os testes executados e seus resultados, assim



como recomendações de medidas de correção e deve possibilitar à CONTRATANTE conhecer suas fragilidades e permitir criar os controles de segurança necessários para minimizar o risco de invasão.

12.10. A CONTRATADA deverá, em caso de impossibilidade por parte da CONTRATANTE de aplicação das mitigações sugeridas, sugerir medidas alternativas de mitigação de risco.

12.11. A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE;

12.12. A CONTRATADA deverá minimamente tentar a evasão de regras do firewall, acesso a roteadores, sistemas operacionais e demais serviços de redes, captura de senhas, etc.

12.13. A CONTRATADA deverá realizar ataques de man in the middle (ARP Spoofing, captura de informações trafegando na rede) e tentativas de burlar firewall para a saída de informações.

12.14. A CONTRATADA deverá realizar dois tipos de teste de intrusão: tentativa de intrusão/penetração através do ambiente interno e tentativa de intrusão através do ambiente externo;

12.15. A CONTRATADA deverá realizar os testes de intrusão/penetração externos, baseando-se nos endereços (URL's) e ranges de IP's públicos da CONTRATANTE registrados no registro.br e NIC.br.



- 12.16. Deverá a CONTRATADA realizar os testes de intrusão/penetração externos, de forma a explorar possíveis vulnerabilidades nos serviços disponíveis.
- 12.17. A CONTRATADA deverá testar servidores, estações e outros equipamentos da estrutura da rede conforme aprovação e indicação da CONTRATANTE, com o objetivo de obter acesso a informações controladas de acordo com quantitativos informados na Tabela 1.
- 12.18. A CONTRATADA deverá testar ativos de rede das unidades da CONTRATANTE, como por exemplo estações de trabalho, roteadores e switches gerenciáveis, de acordo com amostragem de referência informada no ANEXO I e definida pela CONTRATANTE.
- 12.19. Os alvos dos "Testes de Invasão", bem como as premissas e condições para realização dos mesmos serão definidas e aprovadas pelo CONTRATANTE. Todas as fases dos "Testes de Invasão" poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE, haja vista a necessidade de manter a disponibilidade dos ambientes, ativos e serviços do ambiente operacionais.
- 12.20. Os Testes deverão ser realizados, minimamente, por meio das seguintes abordagens: tentativa de intrusão na camada da rede e tentativa de intrusão na camada do aplicativo;
- 12.21. Os Testes de Intrusão poderão ser direcionados aos servidores Web e respectivas aplicações do serviço de hospedagem contratado pela CONTRATANTE;



12.22. A equipe responsável para execução dos testes, deverá ter comprovadamente no mínimo 5 CVE's publicadas nos últimos 5 anos, com pelo menos uma de alta criticidade.

13. TESTES DE INVASÃO EM APLICAÇÕES WEB CONTINUO E RECORRENTE

13.1. Deverão ser realizados testes de invasão do tipo "Cross Site Scripting (XSS)".

13.2. Deverão ser realizados testes de invasão do tipo "Injeção de Código";

13.3. Deverão ser realizados testes de invasão do tipo "Inclusão Remota de Arquivos (RFI)";

13.4. Deverão ser realizados mapeamentos e sondagens, com o objetivo de identificar possíveis vetores de entradas de ataques;

13.5. Deverão ser realizados testes de invasão do tipo "Referência Direta a Objetos";

13.6. Deverão ser realizados testes de invasão do tipo "Vazamento de informações", onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda;

13.7. Deverá ser realizado testes de invasão baseado em "Gerenciamento de Sessões";



- 13.8. Deverão ser analisadas, pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10;
- 13.9. Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações;

14. SOLUÇÃO WEB APPLICATION FIREWALL (WAF)

- 14.1. Dentro da solução de WAF que será provida deverá permitir a análise de tráfego em alto volume permitindo aplicação de correção e mitigação na camada de aplicação, usando as boas práticas no mínimo sobre as top vulnerabilidades do OWASP e estará disponível na camada de EDGE Computing, ou seja, antes da infraestrutura hospedada em nuvem ou em datacenter próprio ou instalada em equipamentos locais “on premises” do ambiente, garantindo o isolamento antes de impactar a infraestrutura da SPTRANS.
- 14.2. Deverá permitir a geração de log de eventos para análise e revisão de regras para a decisão de bloqueio e ajuste.
- 14.3. Deverá ter o monitoramento em regime 24 x 7 pela equipe do SOC a fim de monitorar, suportar e tomar ação de mitigação de risco.
- 14.4. Deverá ter como característica técnica preponderante a atualização das configurações de segurança em tempo real para que qualquer ajuste de proteção necessária nos parâmetros possa começar a rodar imediatamente sem tempo de rollout nos pontos de presença.



- 14.5. O produto fornecido precisará ter a característica de duplo firewall de aplicação (dual WAF) o que garantirá a SPTRANS 02 camadas de parametrizações de segurança diferentes de forma simultânea por instância.
- 14.6. O produto de CDN (content delivery network) associado ao WAF a ser contratado deverá conter pelo menos 03 plataformas de tráfego de conteúdo exclusivas para cada tipo de transmissão de dados, uma para conteúdo estático, outra para o conteúdo dinâmico e uma terceira para as informações financeiras (PCI). Estas 03 camadas de aceleração de conteúdo protegidas pelo WAF deverão ser independentes para a maior segurança.
- 14.7. O Volume do CDN deve suportar no mínimo 10 TB de tráfego mensal sem cobrança de qualquer valor excedente.

15. CONDIÇÕES PARA EXECUÇÃO DO TRABALHO

- 15.1. Deverá a CONTRATADA obedecer a cronologia e ordenar o nível de criticidade de vulnerabilidades detectadas durante as varreduras, para geração de relatórios;
- 15.2. Deverá elaborar e aplicar testes de Engenharia Social através de campanhas de "phishing tests" de forma semestral, para uma amostragem mínima de 300 (trezentos) usuários por teste à ser realizado, apresentando os resultados dos testes e indicar estratégia de melhores práticas para aumento de conscientização dos colaboradores da SPTRANS e como o tema pode ser melhor abordado;
- 15.3. Fornecer suporte e orientação na utilização de ferramenta que adotada e esclarecer quaisquer detalhes das operações de varredura de vulnerabilidades

e/ou relatórios gerados pelos testes em caso de dúvidas tanto da CONTRATANTE, quanto de terceiros envolvidos;

- 15.4. Deverá a CONTRATADA revisar as regras de firewall, validar e apontar melhorias nas regras existentes no ambiente atual da CONTRATANTE, de acordo com o que rege as melhores práticas de segurança da informação;
- 15.5. A CONTRATADA deverá revisar acessos e credenciais administrativas do ambiente de firewall atual, informando sobre melhorias necessárias;
- 15.6. Deverá a CONTRATADA revisar acessos VPN (site-to-site e client-to-site) do ambiente atual da CONTRATANTE, pontuando melhorias de acordo com as melhores práticas de segurança da informação;
- 15.7. A CONTRATADA deverá efetuar testes de malware de forma controlada para avaliar as proteções contra código malicioso do ambiente e propor ajustes e melhorias para elevar a segurança da infraestrutura da CONTRATANTE.

16. EXPERIÊNCIA EXIGIDA DA CONTRATADA

- 16.1. A SPTTrans exigirá atestado(s) ou certidão(ões) emitido(s) em nome da licitante, por pessoa(s) jurídica(s) de direito público ou privado que comprove(m) a execução;
- 16.2. Serviços de segurança de tecnologia da informação para clientes que possuam transações online e em tempo real no volume de 26 milhões de transações por dia, o que corresponde a 50% das transações ocorridas atualmente em nossos sistemas;
- 16.3. Serviços de investigação criminal digital e análise forense digital em ambiente computacional;



16.4. Serviços de monitoramento em operações de NOC/SOC com, pelo menos, 400 mil eventos monitorados por mês.

17. ACORDO DE NÍVEL DE SERVIÇO PARA DISPONIBILIDADE DA SOLUÇÃO DE ANÁLISE DE VULNERABILIDADE

17.1. Qualquer problema relativo à ferramenta de análise de vulnerabilidades que cause interrupção de serviços ou impacte o ambiente durante algum processo de verificação, será imediatamente relatada pela CONTRATANTE;

17.2. Deverá a CONTRATADA reportar à CONTRATANTE qualquer necessidade de manutenção e/ou atualização da ferramenta de varredura de vulnerabilidades, informando a duração e o impacto que causará no processo de seus serviços ou nos dados coletados anteriormente;

17.3. Qualquer relato ou informativo de manutenção deverá ser caracterizado por meio de abertura de chamado: data e horário a partir do qual a CONTRATADA comprovadamente seja acionada, através de Portal Web, telefone ou e-mail a ser definido.

18. NÍVEL DE SERVIÇOS

18.1. Vulnerabilidades críticas encontradas a partir do monitoramento do SIEM e análise de vulnerabilidades encontradas no processo de SCAN pelo SOC



SERVIÇO DE ANÁLISE e ABERTURA DE CHAMADO POR CRITICIDADE			
Prioridade	Tempo de análise para direcionamento da equipe da SPTRANS até:	Validação da correção até:	Situações Cobertas
Critica	2 horas	4 horas	Alto risco de parada, vazamento de informações em ambiente crítico.
Média	4 horas	8 horas	Medio Risco, impacto individual em um ambiente de baixo impacto ao negócio.
Baixa	8 horas	24 horas	Baixo Risco ao negócio ou aceitável a ser tratado pela equipe com base em procedimentos conhecidos e documentados.
SLA de Disponibilidade			
Serviço	Tempo indisponibilidade mensal	Observação.	
SIEM	4 horas	Indisponibilidade da Plataforma.	
SCAN	8 horas	Indisponibilidade do SCAN no processo de execução.	

19. SUPORTE TÉCNICO DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES.

19.1. Deverá a CONTRATADA prover todo o suporte técnico das soluções adotadas, desde a sua implantação, durante a operação e em eventuais manutenções ou atualizações que as ferramentas utilizadas para a prestação do serviço venham sofrer sem custo adicional a SPTRANS.

19.2. PRODUÇÃO DE RELATÓRIOS

19.2.1. A CONTRATADA deve emitir relatórios de vulnerabilidades com os resultados encontrados nas varreduras efetuadas no ambiente da SPTRANS;

19.2.2. A CONTRATADA deverá apresentar os modelos de relatórios, com uma lista de relatórios prontos;

19.2.3. A solução deve permitir a exportação de seus relatórios nos seguintes formatos: PDF, XML, CSV, XLSX, MHTML;



19.2.4. A solução deve possuir em sua gama de relatórios pelo menos os seguintes relatórios:

- 19.2.4.1. Sumário Executivo: Este relatório deve apresentar um resumo do ambiente atual;
- 19.2.4.2. Vulnerabilidade: Este relatório deve detalhar a lista de vulnerabilidades descobertas agrupadas por vulnerabilidade. O relatório deve incluir minimamente os seguintes detalhes sobre cada vulnerabilidade: descrição, como corrigir, referências, pontuação CVSS, última data de descoberta e uma lista de ativos afetados;
- 19.2.4.3. Vulnerabilidades excluídas: Este relatório exibe ativos que tiveram vulnerabilidades excluídas, incluindo a razão da exclusão;
- 19.2.4.4. Compliance de ativos mensal: Este relatório deve apresentar as tendências de conformidade de ativos em seus agrupamentos;
- 19.2.4.5. Scorecard de Vulnerabilidades: Este relatório deve detalhar a idade da gravidade da vulnerabilidade e contagem no scorecard;
- 19.2.4.6. Matriz de Riscos por Vulnerabilidades: Este relatório deve detalhar o risco pelo impacto CVSS agrupado pela contagem de vulnerabilidades;
- 19.2.4.7. Matriz de Riscos por Ativos: Este relatório deve detalhar o risco pelo impacto CVSS agrupado por ativos.

19.3. Integrações necessárias para solução de varredura de vulnerabilidades

- 19.3.1. A solução deverá possuir capacidade de integração com o serviço de diretório LDAP;
- 19.3.2. A solução deverá possuir capacidade de integração com o serviço de diretório Microsoft Active Directory.



19.3.3. A solução deverá possuir, sem necessidade de desenvolvimento, conectores prontos para envio de dados as plataformas de SIEM inclusa na solução do serviço.

19.4. Manutenção da solução de varredura de vulnerabilidades

19.4.1. Por se tratar de um ambiente SaaS e gerenciado pela CONTRATADA, a CONTRATADA deverá fazer a manutenção da solução, bem como corrigir bugs, vulnerabilidades, atualizações e eventuais problemas que forem identificados de forma proativa e na maior transparéncia de esforço e responsabilidade;

19.4.2. Eventuais manutenções na ferramenta de varredura de vulnerabilidades e do SIEM será de responsabilidade da CONTRATADA, que deverá notificar a CONTRATANTE para agendamento da Manutenção Programada para envolver os recursos necessários entre às empresas para a atividade;

19.4.3. Caberá à CONTRATADA notificar a CONTRATANTE caso haja alguma indisponibilidade do serviço prestado.



ANEXO I

AMBIENTE A SER MONITORADO NO SOC

Escopo de volume de ativos base para as seguintes ferramentas :

- Auditoria, Monitoria e Gestão do Active Directory e File Server.
- Gerenciamento, Descoberta e Distribuição de Patches
- SIEM
- SCAN
- Penetration Test.

Descrição	Quantidade
AD/Auth, DHCP, DNS, ESX, O365	25
Web and Mail Servers, O365	12
Windows General Purpose Servers	328
Antivírus, Anti-Malware Servers	4
Database Servers	27
Proxy Servers, Edge/Small Firewalls	12
Core/Large Firewalls	11
IDS, IPS, VPN, WAF, DAM, DLP, LB	9
Routers, Switches, Wireless	290
Servidores não especificados	172
WAF	1
URLS:\Application	20
Estações de Trabalho	1600
Usuário no AD	2500
Localidades Datacenter	3
Volume de horas mínima do RedTeam - Ethical Hacker por URL por mês	80
Volume de eventos mês do WAF para integração do SIEM	10.000.000.000
Volume de horas para investigação digital forense por ano	200
CDN - TB trafegados por mês esperado	10



**ANEXO III
PLANILHA DE QUANTIDADES
E PREÇOS**



LICITAÇÃO Nº 010/2022

ANEXO III - PLANILHA DE QUANTIDADES E PREÇOS (MÓDULO)

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PERÍODO DE 60 (SESSENTA) MESES.

Valores em Reais (R\$)

EXTENSO (VINTE E TRÊS MILHÕES E SEISCENTOS MIL REAIS)

PROONENTE:	RESPONSÁVEL PELA APROVAÇÃO (PROONENTE):
RAZÃO SOCIAL: KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A.	NOME: LEONARDO APARECIDO FIGUEIREDO CABRAL
CNPJ: 05.761.098/0001-13	CARGO: DIRETOR ADMINISTRATIVO
ENDERECO: R. MARIA TERESA DIAS DA SILVA, 270, CAMPINAS/SP - CEP 13.083-820	TELEFONE: 19 3 9233-3500
TELEFONE: 19 3112-5000	

LEONARDO APARECIDO
FIGUEIREDO CABRAL:31972564846

Assinado de forma digital por LEONARDO
APARECIDO FIGUEIREDO CABRAL:31972564846
Dados: 2022.08.16 05:25:54 -03'00'

ANEXO IV
COMPOSIÇÃO DA TAXA DE
BDI



LICITAÇÃO Nº 010/2022
ANEXO IV - COMPOSIÇÃO DA TAXA DE BDI - MODELO

(BENEFÍCIOS E DESPESAS INDIRETAS)

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTTRANS NO DIRECIONAMENTO DO RASTREAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PÉRIODO DE 60 (SESSENTA) MESES

DESCRÍÇÃO	N
Despesas Indiretas e Administrativas:	
Escritório Central	7,37
Total (X)	7,37
Benefícios:	
Lucro	7,40
Total (Y)	7,40
Tributos obrigatórios:	
PIS	0,65
Cofins	3,00
ISSQN	2,00
CPRB	4,50
Total (T)	10,15

<= Número decimal

$$BDI (\%) = \left\{ \left[\frac{\left(1 + \frac{X}{100} \right) \times \left(1 + \frac{Y}{100} \right)}{\left(1 - \frac{T}{100} \right)} - 1 \right] \times 100 \right\}$$

BDI CALCULADO	28,35%
BDI ADOTADO	28,35%

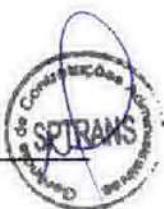
PROONENTE: RAZÃO SOCIAL: KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A. CNPJ: 05.761.098/0001-13 ENDEREÇO: R. MARIA TERESA DIAS DA SILVA, 270 - CAMPINAS/SP - CEP 13.083-820 TELEFONE: 19 3112-5000	DADOS DO RESPONSÁVEL PELA PROONENTE: NOME: LEONARDO APARECIDO FIGUEIREDO CABRAL CARGO: DIRETOR ADMINISTRATIVO TELEFONE: 19 9 9233-3500
--	--

LEONARDO APARECIDO
FIGUEIREDO
CABRAL: [REDACTED]

Assinado de forma digital por LEONARDO
APARECIDO FIGUEIREDO
CABRAL: [REDACTED]
Dados: 2022.08.15 19:40:12 -03'00'



ANEXO V
COMPOSIÇÃO DA TAXA DE
ENCARGOS SOCIAIS



LICITAÇÃO Nº 010/2022

ANEXO V - COMPOSIÇÃO DA TAXA DE ENCARGOS SOCIAIS - MODELO MENSALISTA

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PÉRIODO DE 60 (SESSENTA) MESES

DESCRICAÇÃO	(%)
A - Encargos Sociais	
A 1 - Previdência Social	0,00%
A 2 - FGTS	8,00%
A 3 - Salário Educação	2,50%
A 4 - SEST / SESC / SEST	1,50%
A 5 - SENAI / SENAC / SENAT	1,00%
A 6 - SEBRAE	0,60%
A 7 - INCRA	0,20%
A 8 - Seguro contra risco e acidente de Trabalho (INSS)	2,00%
Total do Grupo (A)	15,80%
B - ENCARGOS QUE RECEBEM INCIDÊNCIA DE (A)	
B 1 - 13º Salário	8,33%
B 2 - Férias	12,10%
B 3 - Faltas Abonadas legalmente	1,20%
B 4 - Aviso Prévio	2,40%
B 5 - Auxílio Enfermidade	0,10%
B 6 - Licença Paternidade	0,10%
Total do Grupo (B)	24,23%
C - ENCARGOS QUE NÃO RECEBEM INCIDÊNCIA GLOBAL DE (A)	
C 1 - Depósito por despedida sem justa causa	3,47%
C 2 - Indenização Adicional (Lei 7.238/84)	0,10%
Total do Grupo (C)	3,57%
D - REINCIDÊNCIAS	
D 1 - Reincidência de A sobre B	3,83%
Total do Grupo D	3,83%
E - COMPLEMENTOS	
E 1 - Vale Refeição	10,00%
E 2 - Vale Transporte	3,00%
E 3 - Seguro de Vida Coletivo	0,20%
Total do Grupo (E)	13,20%
TOTAL DOS ENCARGOS	69,63%

<= Número percentual

<= Optante Desoneração

<= Cálculo automático

PROONENTE:
RAZÃO SOCIAL: KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A.
CNPJ: 05.781.098/0001-13
ENDEREÇO: R. MARIA TERESA DIAS DA SILVA, 270, CAMPINAS/SP - CEP 13.083-820
TELEFONE: 19 3112-5000

DADOS DO RESPONSÁVEL PELA PROONENTE:
NOME: LEONARDO APARECIDO FIGUEIREDO CABRAL
CARGO: DIRETOR ADMINISTRATIVO
TELEFONE: 19 9 8233-3500

LEONARDO APARECIDO
FIGUEIREDO CABRAL:31972564846

Assinado de forma digital por LEONARDO
APARECIDO FIGUEIREDO CABRAL:31972564846
Dados: 2022.08.15 19:53:06 -03'00'



ANEXO VI
CRITÉRIO DE PREÇO E
MEDIÇÃO



LICITAÇÃO Nº 010/2022

ANEXO VI – CRITÉRIO DE PREÇO E MEDIÇÃO

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PERÍODO DE 60 (SESSENTA) MESES

DESCRIÇÃO:

- **SOC MONITORAMENTO 24 X 7 SOC/SIEM**
Unidade: EPS
Quantidade: Anexo I do TR (60 meses)
- **SOC SCAN VULNERABILIDADE**
Unidade: Volume de Ativos
Quantidade: Anexo I do TR (60 meses)
- **SOLUÇÃO DE AUDITORIA, GESTÃO, AUTOMAÇÃO, MONITORAÇÃO E PREVENÇÃO INTERNA**
Unidade: Volume de Usuários
Quantidade: Anexo I do TR (60 meses)
- **PROTEÇÃO AVANÇADA ZERODAY SYSCAL LINUX**
Unidade: Volume de Host Linux
Quantidade: Anexo I do TR (60 meses)
- **SOLUÇÃO PARA AUTOMAÇÃO, GESTÃO, DESCOBERTA, IMPLEMENTAÇÃO E INVENTARIO DE PATCHS EM AMBIENTE DE SERVIDORES E ESTACOES DE TRABALHO COMTEMPLANDO SISTEMAS OPERACIONAIS MICROSOFT E LINUX.**
Unidade: Volume de Ativos
Quantidade: Anexo I do TR (60 meses)
- **TESTE DE PENETRAÇÃO MANUAL**
Unidade: Quantidade
Quantidade: Anexo I do TR (60 meses)
- **MONITORAMENTO MARCA SPTRANS**
Unidade: Volume de Marca atendido
Quantidade: Anexo I do TR (60 meses)
- **WAF + CDN**
Unidade: Volume de Aplicações
Quantidade: Anexo I do TR (60 meses)
- **INVESTIGAÇÃO DIGITAL FORENSE - 200 HORAS POR ANO**
Unidade: Horas (h)



Quantidade: Anexo I do TR (1.000 Horas)

• **TREINAMENTO WORKSHOP VIRTUAL - SEMESTRAL (10)**

Unidade: Quantidade

Quantidade: Item 4.4 do TR (10 Semestres)

PRELIMINARES:

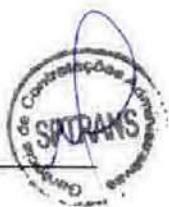
Trata-se de Fornecimento de Serviços Gerenciados de Segurança da Informação, Varredura de Vulnerabilidades, Testes de intrusão/Penetração e Geração de Relatórios, conforme condições e especificações contidas no Termo de Referência e/ou Contrato.

Ressaltamos que nos valores apresentados deverão contemplar, além do lucro, as despesas relativas à:

- ✓ Salários acrescidos dos respectivos encargos e benefícios sociais, instituídos por Lei ou acordo salarial da categoria, de todo o pessoal envolvido direta e indiretamente;
- ✓ As instalações e sua manutenção, mão de obra, materiais, ferramentas, softwares e equipamentos destinados à execução dos serviços e à operacionalização administrativa da CONTRATADA;
- ✓ Comunicações compreendendo telefone, celular, rádio comunicador, fax, internet e correio;
- ✓ EPI's e uniformes, se necessários;
- ✓ Refeições, transportes e mobilizações;
- ✓ Todos os tributos e encargos legais devidos;
- ✓ Seguros e auxílios de qualquer natureza;
- ✓ Demais despesas econômicas não especificadas acima;

MEDIÇÃO:

A medição será realizada mensalmente, de acordo com os itens efetivamente executados conforme os critérios definidos no Termo de Referência e, mediante aprovação da SPTTrans.



ANEXO VIII
CARTA PROPOSTA
COMERCIAL E
PRORROGAÇÃO DA
PROPOSTA



LICITAÇÃO N° 010/2022**ANEXO VIII - CARTA PROPOSTA COMERCIAL**

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PERÍODO DE 60 (SESSENTA) MESES.

Campinas/SP, 16 DE AGOSTO de 2022

SÃO PAULO TRANSPORTE S/A - SPTrans
Rua Boa Vista, nº 236 – 2º andar - Centro CEP 01014-000 - São Paulo – SP

Assunto: PROPOSTA COMERCIAL - AJUSTADA

Prezados senhores,

Apresentamos os preços e condições para o atendimento do objeto acima, conforme regras estabelecidas neste Edital.

1. O Valor Global é o constante da **Planilha de Quantidades e Preços**, preenchida conforme regras estabelecidas neste Edital.
2. A data base dos preços apresentados é a data da apresentação das propostas;
3. Prazo de validade da proposta é de 60 (sessenta) dias a contar da entrega.
4. **QUALIFICAÇÃO/IDENTIFICAÇÃO DA PROPONENTE/LICITANTE:**

LICITAÇÃO N.º 010/22 - São Paulo Transporte S.A. - SPTrans	CARIMBO CNPJ
EMPRESA: Kryptus Segurança da Informação S.A.	05.761.098/0001-13
ENDEREÇO: Rua Maria Tereza Dias da Silva, 270 – Campinas-SP	KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A.
CEP: 13.083-820	Rua Maria Tereza Dias da Silva, 270 Cidade Universitária - CEP: 13083-820 CAMPINAS - SP
TELEFONE: (19) 3112-5000	
FAX: (19) 3112-5000	
CNPJ: 05.761.098/0001-13	
INSCRIÇÃO ESTADUAL: 244.942.208.110	



5. QUALIFICAÇÃO DO REPRESENTANTE LEGAL:

NOME: Leonardo Aparecido Figueiredo Cabral

CPF/MF: 319.725.648-46

CARGO/FUNÇÃO: Diretor Administrativo

RG/IDENTIDADE: 28.546.330-5

EXPEDIDO: SSP/SP NAT/NAC: São Paulo/Brasileiro

Campinas/SP, 16 DE AGOSTO 2022

**LEONARDO APARECIDO
FIGUEIREDO
CABRAL**

**Leonardo Aparecido Figueiredo Cabral
Diretor Administrativo**



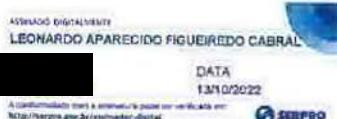
PRORROGAÇÃO CARTA PROPOSTA
LICITAÇÃO Nº 010/2022

Assunto: **PRORROGAÇÃO CARTA PROPOSTA**

OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCO E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PERÍODO DE 60 (SESSENTA) MESES.

A **KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A.**, inscrita no CNPJ 05.761.098/0001-13, situada na Rua Maria Tereza Dias da Silva, 270 – Bairro: Cidade Universitária – Cidade de Campinas/SP – CEP13083-820, por seu representante legal, Sr. Leonardo Aparecido Figueiredo Cabral - RG: 28.546.330-5 - CPF: 319.725.648-46, DECLARA que está prorrogando por mais 30 (trinta) dias, o prazo constante ao item 3 do Anexo VIII – Carta Proposta Comercial, do Edital, datada no dia 16 de agosto de 2022.

Campinas/SP, 13 de outubro de 2022.



Leonardo Aparecido Figueiredo Cabral
Diretor Administrativo
[Redacted]



COMPOSIÇÕES DE PREÇOS UNITÁRIOS



SPTRANS	COMPOSIÇÃO DE PREÇO UNITÁRIO				DATA BASE:	ITEM N°	UNIDADE:	FOLHA N°				
DISCRIMINAÇÃO												
OBJETO: CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, COMPREENDENDO O MONITORAMENTO DE COMPORTAMENTOS QUE APRESENTEM RISCOS E VULNERABILIDADES EM REGIME 24X7, SUPORTAR A SPTRANS NO DIRECIONAMENTO DO RITAMAMENTO DE INCIDENTES DE SEGURANÇA, TREINAMENTO DA EQUIPE E SUPORTE A IMPLANTAÇÃO DE BOAS PRÁTICAS, PELO PERÍODO DE 60 (SESSENTA) MESES												
NOME DA EMPRESA:												
KRYPTUS SEGURANÇA DA INFORMAÇÃO S.A.												
COMPONENTES DO CUSTO		QTD	COEF.	CUSTO UNITÁRIO	PARCELAS DO CUSTO UNITÁRIO X COEF.							
MÃO-DE-OBRA:					MÃO-DE-OBRA	MATERIAL	EQUIPAMENTO	OUTROS				
ITEM 1: SOC MONITORAMENTO 24 X 7 SOC/SIEM		MÊS	60	55.615,96	3.337.018,80							
ITEM 2: SOC SCAN VULNERABILIDADE		MÊS	60	5.563,26	333.795,60							
ITEM 3: SOLUÇÃO DE AUDITORIA, GESTÃO, AUTOMAÇÃO, MONITORAÇÃO E PREVENÇÃO INTERNA		MÊS	60	5.734,67	344.080,20							
ITEM 4: PROTEÇÃO AVANÇADA ZERODAY SYSCAL LINUX		MÊS	60	1.401,90	84.150,00							
ITEM 5: SOLUÇÃO PARA AUTOMAÇÃO, GESTÃO, DESCOPERTA, IMPLEMENTAÇÃO E INVENTÁRIO DE PATCHES EM AMBIENTE DE SERVIDORES E ESTAÇÕES DE TRABALHO CONTEMPLANDO SISTEMAS OPERACIONAIS MICROSOFT E LINUX		MÊS	60	8.103,34	486.200,40							
ITEM 6: TESTE DE PENETRAÇÃO MANUAL		MÊS	60	34.174,29	2.050.457,40							
ITEM 7: MONITORAMENTO MARCA SPTRANS		MÊS	60	1.059,67	63.580,20							
ITEM 8: WAF + CDN		MÊS	60	1.571,25	154.275,00							
ITEM 9: INVESTIGAÇÃO DIGITAL FORENSE - 200 HORAS POR ANO		HORAS	1000	155,91	155.910,00							
ITEM 10: TREINAMENTO WORKSHOP VIRTUAL - SEMESTRAL [10]		SEMESTRE	10	11.687,395	116.873,95							
MATERIAL (SOFTWARES):												
ITEM 1: SOC MONITORAMENTO 24 X 7 SOC/SIEM		MÊS	60	73.724,83		4.423.489,80						
ITEM 2: SOC SCAN VULNERABILIDADE		MÊS	60	10.799,26		647.955,60						
ITEM 3: SOLUÇÃO DE AUDITORIA, GESTÃO, AUTOMAÇÃO, MONITORAÇÃO E PREVENÇÃO INTERNA		MÊS	60	30.107,03		1.806.421,80						
ITEM 4: PROTEÇÃO AVANÇADA ZERODAY SYSCAL LINUX		MÊS	60	7.947,51		476.850,00						
ITEM 5: SOLUÇÃO PARA AUTOMAÇÃO, GESTÃO, DESCOPERTA, IMPLEMENTAÇÃO E INVENTÁRIO DE PATCHES EM AMBIENTE DE SERVIDORES E ESTAÇÕES DE TRABALHO CONTEMPLANDO SISTEMAS OPERACIONAIS MICROSOFT E LINUX		MÊS	60	92.413,37		1.944.802,20						
ITEM 6: TESTE DE PENETRAÇÃO MANUAL		MÊS	60	5.563,26		333.795,60						
ITEM 7: MONITORAMENTO MARCA SPTRANS		MÊS	60	12.186,18		731.170,80						
ITEM 8: WAF + CDN		MÊS	60	14.570,43		874.225,80						
ITEM 9: INVESTIGAÇÃO DIGITAL FORENSE - 200 HORAS POR ANO		HORAS	1000	23,30		23.300,00						
EQUIPAMENTOS:												
OUTROS:												
BOI:												
ESCRITÓRIO CENTRAL (7,37%)					525.211,37	830.010,30	-	-				
LUCRO (7,4%)					886.214,92	884.809,66	-	-				
IMPOSTOS (10,15%)					918.326,51	1.467.071,19	-	-				
SUB TOTAL DAS PARCELAS DO CUSTO UNITÁRIO => => =>					9.146.096,65	14.452.903,35	-	-				
NOTA DA EMPRESA:							PREÇO TOTAL CONTRATO (R\$):					
							23.600.000,00					

LEONARDO APARECIDO FIGUEIREDO CABRAL
DIRETOR ADMINISTRATIVO

LEONARDO APARECIDO
FIGUEIREDO
CABRAL [REDACTED]

Assinado de forma digital por
LEONARDO APARECIDO
FIGUEIREDO CABRAL [REDACTED]
Dados: 2022.08.16 07:08:51 -03'00'

