CONTRATO Nº 2022/0280-01-00 PARA FORNECIMENTO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, VARREDURA DE VULNERABILIDADES, TESTES DE INTRUSÃO/PENETRAÇÃO E GERAÇÃO DE RELATÓRIOS, QUE ENTRE SI CELEBRAM, A "**SÃO PAULO TRANSPORTE S/A**" E A EMPRESA **"BRASTORAGE COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA. (THINK ABOUT IT)"**, NA FORMA ABAIXO MENCIONADA:

SÃO PAULO TRANSPORTE S/A
Gerência de Contratações Administrativas
Registro N.º 2022/0280-01-00

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, 236, cadastrada no CNPJ/MF sob n° 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 **"SPTrans"**, e de outro a empresa **BRASTORAGE COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA. (THINK ABOUT IT)**, com sede na cidade de São Paulo, na Av. Maria Coelho Aguiar, 215 – Bloco C - 4° andar - Jardim São Luís, cadastrada no CNPJ/MF nº 08.053.426/0001-15, neste ato representada por seus Sócios ao final nomeados e qualificados, que também subscrevem3 o presente, doravante denominada simplesmente **CONTRATADA**; contratação emergencial vinculada ao Processo Administrativo de Licitações e Contratos - PALC nº **2022/0280-01-00**, com fundamento no artigo 29, XV, da Lei Federal nº 13.303/2016 e no artigo 175, XV, do RILC da SPTrans, 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 e pelo Código de Conduta e Integridade da **SPTrans**, disponível no link http://dados.prefeitura.sp.gov.br/dataset/codigo-de-conduta-e-integridade-sptrans, e em conformidade com a Resolução da Diretoria da SPTrans nº 22/054 de 10 de maio de 2022 (SEI 5010.2022/0005776-3), e, demais diplomas aplicáveis à espécie, têm justo e avençado o seguinte:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. Constitui objeto do presente contrato o fornecimento de serviços gerenciados de segurança da informação, varredura de vulnerabilidades, testes de intrusão/penetração e geração de relatórios.

CLÁUSULA SEGUNDA - DOS DOCUMENTOS INTEGRANTES

2.1. Integram o presente contrato tal como se nele transcritos os documentos a seguir relacionados:

2.1.1. **Anexo I** – Termo de Referência;

2.1.2. **Anexo II** - Proposta Comercial nº 2836599308.2022-1, da **CONTRATADA** de 19 de abril de 2022;

2.1.2.1. Na hipótese de divergência de redação entre o contrato e a proposta comercial apresentada, prevalecerá a redação contratual.

2.1.3. **Anexo III** – Modelo de Carta de Autorização de Crédito em Conta Corrente.

CLÁUSULA TERCEIRA - DO PRAZO

3.1. O prazo total de vigência deste contrato será de até 180 (cento e oitenta) dias contados de 15/05/2022, podendo ser rescindindo antecipadamente quando se ultimar o regular processo licitatório em andamento.

3.1.1. O início de vigência estabelecido no item 3.1 tem fulcro no artigo 175, inciso XV c/c artigo 182, § 6º, do Regulamento Interno de Licitações e Contratos – RILC da **SPTrans**.

CLÁUSULA QUARTA - DO RECURSO ORÇAMENTÁRIO E FINANCEIRO

4.1. O recurso necessário para suportar a despesa deste instrumento, para o exercício de 2022 consta da "Previsão Orçamentária da SPTrans", conforme Requisição de Compra – RC nº 27.509.

CLÁUSULA QUINTA - DO VALOR

5.1. Tem o presente contrato o valor total de R$ 2.522.587,20 (dois milhões, quinhentos e vinte e dois mil, quinhentos e oitenta e sete reais e vinte centavos), referido ao mês da data da apresentação da proposta, ou seja, abril/2022.

CLÁUSULA SEXTA – DA EXECUÇÃO CONTRATUAL

6.1. Para a execução do objeto a **CONTRATADA** deverá obedecer às condições descritas nesta Cláusula, bem como às demais condições estabelecidas no presente contrato e no Anexo I – Termo de Referência.

6.2. A **CONTRATADA** deverá obedecer á cronologia e ordenar o nível de criticidade de vulnerabilidades detectadas durante as varreduras, para geração de relatórios.

6.3. A **CONTRATADA** 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 a 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.

6.4. A **CONTRATADA** deverá fornecer suporte e orientação na utilização de ferramenta adotada e esclarecer quaisquer detalhes das operações de varredura de vulnerabilidades e/ou relatórios gerados pelos testes em caso de dúvidas tanto da **SPTrans**, quanto de terceiros envolvidos.

6.5. A **CONTRATADA** deverá revisar as regras de firewall, validar e apontar melhorias nas regras existentes no ambiente atual da **SPTrans**, de acordo com o que rege as melhores práticas de segurança da informação.

6.6. Deverá a **CONTRATADA** revisar acessos VPN (site-to-site e client-to-site) do ambiente atual da **SPTrans**, pontuando melhorias de acordo com as melhores práticas de segurança da informação.

6.7. 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 **SPTrans**.

6.8. Deverá a **CONTRATADA** prover todo o suporte técnico das soluções adotadas, desde o início da operação e em eventuais manutenções ou atualizações que as ferramentas utilizadas para a prestação do serviço venham sofrer obedecendo ao tempo Nível de Serviços (SLA) sem custo adicional a **SPTrans**, conforme descritos nos itens 14 e 15 do Termo de Referência.

6.9. A **CONTRATADA** deverá prover todo serviço de segurança para a infraestrutura de TI da **SPTrans** em regime 24/7, conforme descritos no item 2 do Termo de Referência.

6.10. Deverá a **CONTRATADA** prover um Portal Web, telefone e/ou e-mail, para abertura dos chamados técnicos.

6.11. A execução do Contrato deverá ser acompanhada e fiscalizada por representante da **SPTrans** designado para esse fim.

6.12. A **CONTRATADA** sugerirá à **SPTrans**, em tempo hábil, todas as providências que sejam necessárias à adequação do objeto contratual aos aspectos imprevistos ou supervenientes constatados durante a execução dos serviços, de modo que quaisquer problemas, falhas ou omissões decorrentes dos aspectos acima mencionados possam ser superados pela **SPTrans**, sem o comprometimento da execução do objeto do Contrato.

6.13. Na realização dos serviços, a **CONTRATADA** deverá respeitar as exigências constantes nas especificações técnicas, instruções, projetos, normas técnicas editadas pela ABNT, se citadas explicitamente ou não, e os padrões referenciais da **SPTrans**.

6.13.1. Na falta de normatização, os parâmetros mínimos de qualidade dos serviços serão definidos pela **SPTrans**.

6.14. Caso a **CONTRATADA** identifique a necessidade de execução de serviços não constantes do orçamento preliminar, deverá submeter solicitação à aprovação prévia da **SPTrans**.

6.15. Caso venha a ocorrer a necessidade de providências complementares por parte da **SPTrans**, a fluência do prazo de vigência será interrompida, reiniciando-se a sua contagem a partir da data em que estas forem cumpridas.

CLÁUSULA SÉTIMA – DOS PREÇOS

7.1. Para todos os serviços, objeto deste contrato, serão adotados os preços unitários, fixos e irreajustáveis, propostos pela **CONTRATADA** constantes no Anexo II – Proposta Comercial, referido ao mês da data de sua apresentação, ou seja, abril/2022.

7.2. Nos preços unitários propostos que constituirão a única e completa remuneração para o fornecimento objeto do contrato, estão computados todos os custos, tributos e despesas da **CONTRATADA**, nada mais podendo a **CONTRATADA** pleitear a título de pagamento, reembolso ou remuneração em razão do contrato, de sua celebração e cumprimento.

7.3. 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.

7.4. 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.

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, 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 um mês a partir da data de término da medição anterior, exceto a medição final, que poderá abranger menor período, por se tratar do último da execução do objeto.

8.1.3. Para efeito do cálculo pro-rata considerar-se-á mês comercial de 30 (trinta) dias.

8.2. Realizada a medição, a **CONTRATADA** enviará o respectivo relatório dos serviços à **SPTrans** até o 1º (primeiro) dia útil subseqüente ao término da prestação de serviço, sendo que a **SPTrans** terá o prazo de 02 (dois) dias úteis do recebimento, para aceitá-la.

8.2.1. Se a **CONTRATADA** não apresentar a medição do período, dentro dos prazos previstos, sua análise/liberação para processamento se dará concomitantemente com a medição do mês subseqüente.

8.2.2. A **CONTRATADA** estará autorizada a emitir Nota Fiscal/Fatura (documento de cobrança), após a aceitação formal da **SPTrans** da medição apresentada, em conformidade com os prazos estabelecidos.

8.2.3. A **CONTRATADA** deverá emitir Nota Fiscal em separado, de acordo com o valor e respectiva fonte de recurso, informados pela **SPTrans**, na aceitação formal da medição.

8.2.4. No 1º dia útil do mês subsequente, a **CONTRATADA** emitirá uma única Nota Fiscal/Fatura referente aos serviços prestados no mês anterior.

8.3. Os pagamentos referentes às medições, quando devidos, serão efetuados 30 (trinta) dias após a data de apresentação e aceite pela **SPTrans** das Notas Fiscais/Faturas dos serviços, por meio de crédito em conta corrente que a **CONTRATADA** deverá manter no banco indicado pela **SPTrans**.

8.3.1. 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 – Centro – São Paulo – SP, conforme Anexo III - Modelo de Carta de Autorização de Crédito em Conta Corrente.

8.3.2. Caso a **CONTRATADA** solicite que o pagamento seja creditado em conta corrente de outro banco que não o indicado pela **SPTrans**, arcará com todas as despesas e tarifas bancárias vigentes, incorridas na transação de pagamento: DOC, TED, Tarifa de emissão de Cheque e outras.

8.3.3. A efetivação do pagamento à **CONTRATADA** fica condicionada à ausência de registro no CADIN – Municipal, nos termos da Lei Municipal nº. 14.094/05.

8.3.4. No caso de eventual atraso no pagamento pela **SPTrans**, o valor devido será atualizado financeiramente, *pró-rata temporis*, desde o dia do 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. Para efeito deste cálculo considerar-se-á mês comercial de 30 (trinta) dias.

8.3.4.1. Essa atualização não será aplicada, na hipótese de suspensão do pagamento, em razão do cumprimento da Lei Municipal nº 14.094/2005, caso a **CONTRATADA** esteja inscrita no CADIN Municipal.

8.4. As Notas Fiscais/Faturas (documentos de cobrança) emitidas pela **CONTRATADA** deverão mencionar os seguintes dados:

8.4.1. Endereço: Rua Boa Vista, 236 – Centro - CEP 01014-000 – São Paulo/SP;

8.4.2. CNPJ: 60.498.417/0001-58; Inscrição Estadual: (Isenta);

8.4.3. Número de registro deste contrato e/ou item contratual (quando for o caso) e a data de sua assinatura;

8.4.4. Objeto Contratual;

8.4.5. O endereço de entrega da Nota Fiscal/Fatura será aquele que o gestor do contrato, no âmbito da **SPTrans**, designar;

8.4.6. O valor correspondente à retenção do Imposto de Renda Retido na Fonte (IRRF), das Contribuições Sociais (PIS/COFINS/CSLL) e do Imposto Sobre Serviço (ISS), bem como a respectiva base de cálculo, em relação ao serviço de suporte técnico.

8.4.7. O valor correspondente à retenção do Imposto Sobre Serviço (ISS), bem como a respectiva base de cálculo, em relação aos serviços de licenciamento, processamento, armazenamento e comunicação de dados.

8.5. No caso da **CONTRATADA** não ser obrigado a destacar a retenção na fonte dos tributos acima relacionados, deverá discriminar nas Notas Fiscais/Faturas os devidos enquadramentos legais e anexar os documentos comprobatórios.

8.6. 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, conforme legislação em vigor.

8.7. A **CONTRATADA** dará como quitadas as duplicatas e outros documentos de cobrança emitidos contra a **SPTrans**, pela efetivação do crédito em conta corrente.

8.8. Quaisquer outros títulos emitidos pela **CONTRATADA** deverão ser mantidos em carteira, não sendo a **SPTrans** obrigada a efetuar o seu pagamento, se colocados em cobrança pelo sistema bancário.

8.9. Quaisquer pagamentos não isentarão a **CONTRATADA** das responsabilidades contratuais, nem implicarão a aceitação definitiva dos serviços.

8.10. A **SPTrans** poderá descontar de qualquer pagamento, importância que a qualquer título lhe seja devida pela **CONTRATADA**, por força deste contrato, garantidos os princípios do contraditório e ampla defesa, quando for o caso, não podendo ser descontadas importâncias devidas por força de outros contratos.

8.11. Nos termos do artigo 222, § 2º do RILC, a **SPTrans** poderá promover a retenção preventiva de créditos devidos à **CONTRATADA** em função da execução do contrato, quando assim se fizer necessário, para evitar prejuízo decorrente do inadimplemento da **CONTRATADA** de encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

8.12. A retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, poderá ocorrer quando a **CONTRATADA**:

8.12.1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas;

8.12.2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8.12.3. Fórmula e Parâmetros para o cálculo da glosa - GLOSA DO MÊS: A Glosa do Mês será aplicada no mês subsequente. A **SPTrans** informará a **CONTRATADA** até o 5º dia útil do mês o valor da glosa para emissão de Nota Fiscal. Tendo a **CONTRATADA** para recurso, 3 (três) dias para apresentação e a **SPTrans** a partir desse recebimento mais 3 (três) dias para análise, sendo que após a análise e havendo alteração a **CONTRATADA** deverá reapresentar o valor com a glosa no prazo de até 5 (cinco) dias.

Exemplo: Nota fiscal referente o mês de Junho, a Glosa referente a esse mês será apresentada até o 5º (quinto) dia útil do mês de Julho e terá que ser aplicada na emissão da Nota Fiscal do mês de Julho e assim sucessivamente quando houver.

G = (VCL/HM)*TIND onde:

G = Glosa;

VCL = Valor da Parcela Mensal do Contrato;

HM = Quantidade total de horas no mês;

TIND = Tempo de Indisponibilidade.

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

CLÁUSULA NONA - DAS RESPONSABILIDADES E OBRIGAÇÕES

9.1. São obrigações da **CONTRATADA:**

9.1.1. Ter pleno conhecimento das condições, pelo que reconhece ser perfeitamente viável o cumprimento integral e pontual dos encargos assumidos.

9.1.2. Ser responsável pelos danos causados à **SPTrans** ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

9.1.3. A **CONTRATADA** obriga-se a não prestar as informações de qualquer ordem a terceiros, técnicas ou não, sobre a natureza ou andamento da execução dos serviços, filmar, fotografar ou divulgá-los por qualquer outra forma, sem prévia autorização expressa da **SPTrans**.

9.1.3.1. Se a **CONTRATADA** desejar, para fins promocionais ou publicitários, divulgar os serviços a seu cargo, somente poderá

fazê-lo mediante apresentação prévia das mensagens e sua aprovação pela **SPTrans**.

9.1.4. Informar a **SPTrans**, a qualquer tempo, a ocorrência das seguintes situações:

9.1.4.1. Declaração de inidoneidade por ato do Poder Público;

9.1.4.2. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração;

9.1.4.3. Impedimento de licitar, de acordo com o previsto no artigo 9º da Lei Federal nº 8.666, de 21 de junho de 1993 e/ou art. 7º da Lei Federal nº 10.520/02.

9.1.5. Na execução do presente contrato, a **CONTRATADA** estará obrigada a:

9.1.5.1. Executar todos os serviços fielmente, de acordo com as especificações do Termo de Referência - Anexo I deste Contrato, não sendo admitidas quaisquer alterações sem prévio conhecimento e aprovação por parte da **SPTrans**;

9.1.5.2. Não divulgar dados ou informações, nem fornecer cópias de relatórios e documentos a terceiros sem a prévia autorização, por escrito, da administração da **SPTrans**;

9.1.5.3. Assumir inteira responsabilidade técnica pela execução dos serviços, pela confiabilidade e efetividade dos trabalhos que executar;

9.1.5.4. Participar, com representante credenciado em nome da **CONTRATADA**, de todas as reuniões e outras atividades de coordenação, planejamento, acompanhamento e avaliação que venham a ser convocadas pela **SPTrans**;

9.1.5.5. Atender os prazos máximos estabelecidos no Anexo I - Termo de Referência – Apuração de ANS;

9.1.5.6. Respeitar e fazer com que seu pessoal respeite as normas de segurança, higiene e medicina do trabalho;

9.1.5.7. Fornecer todos os recursos humanos, equipamentos e materiais, necessários e suficientes à prestação dos serviços;

9.1.5.8. Responsabilizar-se, inclusive perante terceiros, por ações ou omissões de seus empregados, prepostos e contratados, das quais resultem danos ou prejuízos a pessoas ou bens, não implicando co-responsabilidade da **SPTrans**;

9.1.5.9. Responsabilizar-se pela disciplina, respeito e cortesia dos empregados durante o atendimento técnico, bem como pelo cumprimento das regras e normas internas da SPTrans;

9.1.5.10 Fornecer crachá de identificação, exigindo o uso do mesmo nas dependências da **SPTrans**, para o pessoal designado para execução dos serviços;

9.1.5.11 Substituir, sempre que exigido pela **SPTrans**, qualquer empregado cuja atuação, permanência e/ou comportamento sejam julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão e/ou ao interesse do serviço público;

9.1.5.12. Indicar, por escrito, um representante e substituto eventual, com poderes para resolver todos os assuntos relacionados ao contrato de prestação de serviços.

9.1.5.13. Manter base de conhecimento com todas as informações a respeito do serviço contratado.

9.1.5.14. Designar, no prazo de **10 (dez) dias** a contar da assinatura do presente, responsável pela coordenação técnico-administrativa do contrato, com poderes para tomar as decisões e receber as orientações necessárias ao desenvolvimento adequado dos trabalhos ora contratados, cabendo advertência se não o fizer;

9.1.5.15. Responsabilizar-se pelo estudo de todos os documentos e outros elementos disponibilizados pela **SPTrans** que sejam objeto deste contrato, não se admitindo, em nenhuma hipótese, a alegação de ignorância dos mesmos;

9.1.5.16. Desenvolver todos os trabalhos em regime de colaboração com a **SPTrans**, proporcionando facilidade de acesso a todos os documentos e controles relacionados aos serviços contratados e aos locais onde se encontram os equipamentos dedicados à prestação dos serviços contratados;

9.1.5.17. Observar as práticas de boa prestação empregando somente recursos de melhor qualidade;

9.1.5.18. Providenciar para que os recursos humanos estejam a tempo nas horas e locais determinados pela **SPTrans**;

9.1.5.19. Obedecer e fazer observar as leis, regulamentos, posturas e determinações das autoridades Federais, Estaduais e Municipais, cabendo à **CONTRATADA** integral responsabilidade pelas consequências das eventuais transgressões que, por si ou seus prepostos, cometer, inclusive de natureza ambiental;

9.1.5.20. Se, nos serviços realizados no âmbito de suas atividades específicas a **CONTRATADA** vier a constatar quaisquer discrepâncias, omissões ou erros de natureza técnica ou transgressão às normas técnicas e relativas a direitos autorais e outras, desde que especificamente relacionadas ao objeto contratado, deverá comunicar o fato, por escrito, à **SPTrans**, para

que os mesmos sejam sanados em tempo hábil e suficiente para a continuidade e conclusão dos trabalhos dentro do prazo contratado;

9.1.5.21. Responder única e exclusivamente por quaisquer diferenças, erros ou omissões dos serviços ou outras informações que vier a fornecer;

9.1.5.22. Responsabilizar-se por infração decorrente de fornecimento indevido de tecnologias, programas ou processos protegidos pela Lei de Marcas e Patentes;

9.1.5.23. Alertar a **SPTrans** sobre possíveis interferências técnicas e outras dificuldades que poderão surgir durante a execução dos serviços, as quais deverão ser comunicadas àquela por escrito;

9.1.5.24. Ceder à **SPTrans** todos os códigos-fonte e os direitos de uso sobre os softwares aplicativos e respectivas bibliotecas e manuais de documentação que venha a ter desenvolvidos pela **CONTRATADA** para atender o escopo deste contrato, ressalvado sempre o direito sobre as marcas, patentes registradas e direitos autorais, de propriedade ou titularidade da **CONTRATADA** ou de terceiros, nos termos da legislação aplicável;

9.1.5.25. Manter estrita confidencialidade sobre os documentos, informações, arquivos, códigos-fonte e demais dados pertinentes ao desenvolvimento e execução específicos do objeto ora contratado, em especial aos softwares que constituem o sistema de segurança das transações eletrônicas com os cartões Smart Cards, estendendo esta confidencialidade a seus funcionários, consultores, auditores, e outras pessoas físicas que tenham acesso aos sistemas;

9.1.6. A **CONTRATADA** obriga-se a manter, durante toda a execução dos serviços, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação (artigo 190, inciso XV, do RILC).

9.1.7. A **CONTRATADA** obriga-se a efetivar seguro de seus empregados contra acidente do trabalho, com cobertura do INSS, assumir os ônus decorrentes da legislação trabalhista, previdenciária e acidentária, comprometendo-se como única e exclusiva empregadora e responsável pelo pessoal, bem como deverá manter sempre em vigor, apólices de todos os seguros legalmente obrigatórios, ficando expressamente afastada a existência de qualquer relação de emprego com a **SPTrans**.

9.1.7.1. A inadimplência da **CONTRATADA**, com referência aos encargos referidos no item 9.1.7, não transfere à **SPTrans** a responsabilidade de seu pagamento, nem poderá onerar o objeto do contrato.

9.1.7.2. A **CONTRATADA** deverá ressarcir eventuais prejuízos sofridos pela **SPTrans** em virtude do seu inadimplemento em relação ao cumprimento de encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, incluindo-se nesse dever custas judiciais, honorários advocatícios entre outros regularmente suportados pela **SPTrans**.

9.1.8. 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**.

9.1.9. Nenhum recurso poderá ser retirado ou transferido dos serviços por iniciativa da **CONTRATADA**, sem prévia autorização da **SPTrans**.

9.1.10. Ainda que os serviços estejam concluídos e mesmo que esteja encerrado o prazo contratual, a **CONTRATADA** ficará responsável por quaisquer esclarecimentos que se fizerem necessários, a critério da **SPTrans**.

9.1.11. No caso de utilização de produtos e subprodutos da madeira de origem exótica ou nativa, manter em seu poder cópia autenticada da 1ª (primeira) via da Autorização de Transporte de Produtos Florestais - ATPF, para fins de comprovação da regularidade perante o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis - IBAMA.

9.2. Cumprimento dos requisitos previstos nos incisos I e II do artigo 6º do Decreto Municipal nº 50.977, de 06/11/09, sob pena de rescisão contratual, aplicação de penalidades e sanção administrativa, conforme estabelece o inciso IV do referido decreto.

9.3. Fica ainda, a **CONTRATADA** obrigada a cumprir as seguintes exigências do Decreto Municipal nº 48.184, de 13/03/07.

9.3.1. Utilização de produtos de empreendimentos minerários que tenham procedência legal.

9.3.2. Apresentação, pela **CONTRATADA**, em cada medição, como condição para recebimento das obras ou serviços de engenharia executados, dos seguintes documentos:

9.3.2.1. notas fiscais de aquisição desses produtos;

9.3.2.2. na hipótese de o volume dos produtos minerários ultrapassar 3m³ (três metros cúbicos), cópia da última Licença de Operação do empreendimento responsável pela extração dos produtos de mineração, emitida pela Companhia de Tecnologia de Saneamento Ambiental - CETESB, quando localizado no Estado de São Paulo, ou de documento equivalente, emitido por órgão ambiental competente, integrante do Sistema Nacional do Meio Ambiente - SISNAMA, no caso de empreendimentos localizados em outro Estado.

9.3.3. Pelo descumprimento do disposto neste item, a **CONTRATADA** estará sujeito à rescisão do contrato, com fundamento no artigo 236 e seguintes, e na aplicação das penalidades estipuladas no artigo 241, todos do RILC, e da sanção administrativa de proibição de contratar com a Administração Pública pelo período de até 3 (três) anos, com base no inciso V do § 8º do artigo 72 da Lei Federal nº 9.605, de 12 de fevereiro de 1998, sem prejuízo das implicações de ordem criminal.

9.4. São obrigações da **SPTrans**:

9.4.1. Designar por escrito o gestor para acompanhar e fiscalizar a execução do presente contrato.

9.4.2. Assistir a **CONTRATADA** nas ações judiciais de que venha participar em decorrência deste contrato, na defesa de interesse do trabalho ou comerciais seus, desde que necessário e a juízo da **SPTrans**.

9.4.3. Subscrever, desde que necessários, os requerimentos e expedientes de interesse da **CONTRATADA**, perante as Administrações Direta e Indireta Federal, Estadual e Municipal, sempre limitados ao presente.

9.4.4. Prestar todas as informações e tomar as decisões em tempo hábil, necessárias ao desenvolvimento dos trabalhos pela **CONTRATADA**.

9.4.5. Cumprir os prazos previstos nos itens que se referem à aceitação das medições e nos pagamentos.

CLÁUSULA DÉCIMA - DA FISCALIZAÇÃO DOS SERVIÇOS

10.1. A apresentação da Fiscalização será realizada por meio de documento redigido e assinado pela **SPTrans**, onde constarão, também, as determinações quanto aos trabalhos a serem executados.

10.2. Para permitir a livre atuação dos fiscais, a **CONTRATADA** obriga-se a:

10.2.1. Prestar esclarecimentos e informações solicitadas pela Fiscalização, garantindo o acesso, a qualquer tempo, às suas instalações.

10.2.2. Atender prontamente as reclamações, exigências ou observações feitas pela Fiscalização, refazendo ou corrigindo, quando for o caso e às suas expensas, os serviços que, comprovadamente, não obedecerem às especificações técnicas ou diretrizes da **SPTrans**.

10.2.3. Sustar, a pedido da Fiscalização, ou por livre iniciativa, qualquer parte dos serviços em andamento que, comprovadamente, não estiver sendo executada de acordo com as especificações técnicas.

10.3. Todas as solicitações, reclamações, exigências ou observações relacionadas com o objeto contratado somente produzirão efeito se processadas por escrito.

CLÁUSULA DÉCIMA PRIMEIRA - DA GARANTIA

11.1. A **CONTRATADA** deverá apresentar à **SPTrans** 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.

11.2. A garantia será de R$ 126.129,36 (cento e vinte e seis mil, cento e vinte e nove reais e trinta e seis centavos), 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 a **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. A garantia prestada por meio de seguro-garantia ou carta fiança deverá ter prazo de vigência superior em 90 (noventa) dias à vigência do contrato.

11.4.1. As garantias prestadas na modalidade de fiança bancária ou seguro garantia deverão ser apresentadas 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).

11.4.2. 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.

11.4.3. Constatada qualquer irregularidade na conferência da autenticidade, deverá ser providenciada a imediata substituição da garantia.

11.5. O não recolhimento, pela **CONTRATADA**, da garantia de execução do contrato no prazo estabelecido no item 11.1 caracteriza o descumprimento total da obrigação assumida, sujeitando-a às sanções correspondentes.

11.6. O atraso superior a 25 (vinte e cinco) dias para a apresentação da garantia a que se refere o item anterior, autorizará a **SPTrans** 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. Poderão ser descontadas da garantia, multas impostas à **CONTRATADA**. Se o total da garantia existente for insuficiente, a **CONTRATADA** terá prazo

improrrogável de 48 (quarenta e oito) horas para completar o valor das multas e repor a garantia, a contar da intimação da decisão final, no que concerne às multas.

11.9. 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, pendências trabalhistas, previdenciárias ou de qualquer outra natureza, e ainda, após a assinatura pela **CONTRATADA**, do "Termo de Conclusão, Encerramento e Quitação".

11.10. A garantia de execução contratual poderá ser alterada quando conveniente a sua substituição a pedido da **CONTRATADA** e desde que aceita pela **SPTrans**.

11.11. Para 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, até a data da comunicação à **SPTrans** para sua liberação - nas condições estabelecidas para a matéria em regulamentações expedidas pela Secretaria Municipal de 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, conforme estipulados nesta cláusula, estabelecendo-se o mês comercial de 30 (trinta) dias.

CLÁUSULA DÉCIMA SEGUNDA - DAS ALTERAÇÕES, RESCISÃO, RECURSOS, PENALIDADES, MULTAS E SUSPENSÃO.

12.1. Este contrato, regido pelo RILC, poderá ser alterado qualitativamente 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 **SPTrans**.

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. Na hipótese de alterações contratuais para fins de fixação de preços dos insumos e serviços a serem acrescidos no contrato, deverá ser mantido o mesmo percentual de desconto oferecido pela **CONTRATADA** na licitação.

12.1.4. Se no contrato não foram contemplados preços unitários para obras, serviços ou bens, estes serão fixados mediante acordo entre as partes, respeitado o limite estabelecido no subitem 12.1.2.

12.1.5. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos neste item, 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 5% (cinco por cento) do valor do contrato por atraso na entrega da **garantia contratual**.

12.2.2. Multa pela **inexecução total** do contrato: 20% (vinte por cento) sobre o valor contratual.

12.2.2.1. Entende-se como inexecução total do contrato o não atendimento do pedido de fornecimento, em até 30 (trinta) dias contados da data prevista para o inicio da operação.

12.3. Multas pela inexecução parcial:

12.3.1. Multa de 10% (dez por cento) sobre o valor da parcela não fornecida.

12.3.2. Multa de 2% (dois por cento) por dia de atraso, pela entrega em atraso, não superior a 10 (dez) dias, contados da data prevista para a entrega.

12.3.3. Multa de 2% (dois por cento) pelo não atendimento a exigência do termo de referência.

12.4. As penalidades ora previstas serão aplicadas pela **SPTrans** quando não forem aceitas as competentes justificativas do **CONTRATADA**, devidamente fundamentadas, instruídas em processo administrativo.

12.5. 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.

12.6. A Garantia Contratual, prestada nos termos da Cláusula Décima Primeira, seus itens e subitens, responderá pelas multas aplicadas, por indenizações devidas ou por quaisquer outras pendências contratuais existentes.

12.7. As multas previstas nesta cláusula não têm caráter compensatório, mas simplesmente moratório e, portanto, não exime a **CONTRATADA** da reparação de eventuais danos, perdas ou prejuízos que os seus atos venham a acarretar à **SPTrans** ou a terceiros.

12.8. 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.

12.9. A inexecução total ou parcial do contrato poderá ensejar a sua rescisão, com as consequências cabíveis. Constituirão motivo para rescisão do contrato:

12.9.1. O descumprimento de obrigações contratuais;

12.9.2. A alteração da pessoa do **CONTRATADA**, mediante:

12.9.2.1. 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 **SPTrans**, observado o RILC;

12.9.2.2. A fusão, cisão, incorporação, ou associação da **CONTRATADA** com outrem, não admitidas no contrato e sem prévia autorização da **SPTrans**.

12.9.3. O desatendimento das determinações regulares do gestor ou fiscal do contrato;

12.9.4. O cometimento reiterado de faltas na execução contratual;

12.9.5. A dissolução da sociedade contratada;

12.9.6. A decretação de falência da **CONTRATADA**;

12.9.7. A alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, desde que prejudique a execução do contrato;

12.9.8. Razões de interesse da **SPTrans**, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;

12.9.9. O atraso nos pagamentos devidos pela **SPTrans** decorrentes de obras, serviços ou fornecimentos, ou parcelas destes, já recebidos ou executados, salvo em caso de 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;

12.9.10. A não liberação, por parte da **SPTrans**, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais.

12.9.11. A ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, impeditiva da execução do contrato;

12.9.12. A não integralização da garantia de execução contratual no prazo estipulado;

12.9.13. 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;

12.9.14. O perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença;

12.9.15. 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.

12.10. 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.

12.11. A rescisão do contrato poderá ser:

12.11.1. Por ato unilateral e escrito de qualquer das partes;

12.11.2. Amigável, por acordo entre as partes, reduzida a termo no processo de contratação, desde que haja conveniência para a **SPTrans**;

12.11.3. Judicial, nos termos da legislação.

12.12. A rescisão por ato unilateral a que se refere o subitem 12.11.1 deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 30 (trinta) dias.

12.12.1. Na hipótese de imprescindibilidade da execução contratual para a continuidade de serviços públicos essenciais, o prazo a que se refere o item anterior será de 90 (noventa) dias.

12.13. Quando a rescisão ocorrer sem que haja culpa da outra parte contratante, será esta ressarcida dos prejuízos que houver sofrido, regularmente comprovados, e no caso da **CONTRATADA** terá esta ainda direito a:

12.13.1. Devolução da garantia;

12.13.2. Pagamentos devidos pela execução do contrato até a data da rescisão;

12.13.3. Pagamento do custo da desmobilização.

12.14. A rescisão por ato unilateral da **SPTrans** acarretará as seguintes consequências, sem prejuízo das sanções previstas neste contrato e no RILC:

12.14.1. Assunção imediata do objeto contratado, pela **SPTrans**, no estado e local em que se encontrar;

12.14.2. Execução da garantia contratual, para ressarcimento pelos eventuais prejuízos sofridos pela **SPTrans**;

12.14.3. Na hipótese de insuficiência da garantia contratual, a retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à **SPTrans**;

12.14.4. 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. Não será aceita a subcontratação.

CLÁUSULA DÉCIMA QUARTA - DA FUSÃO, CISÃO E INCORPORAÇÃO

14.1. Poderá ser admitida, mediante prévia aprovação pela **SPTrans**, a fusão, cisão ou incorporação da **CONTRATADA**.

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 **SPTrans**, 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. O gestor e fiscal do contrato devem acompanhar a execução dos serviços contratados, verificando a correta execução dos serviços para que seja mantida a sua qualidade, solicitando, quando for o caso, correção dos mesmos por inadequação; efetuar glosas de medição por serviços mal executados ou não executados, sugerindo a aplicação de penalidades à **CONTRATADA** por inadimplemento contratual; liberação das medições corretas nos prazos previstos para emissão de fatura para pagamento dos serviços prestados.

15.3. Para gerir e controlar a execução do presente contrato, a **SPTrans** designa a Superintendência de Tecnologia da Informação e Comunicação – DG/STI.

15.4. Os responsáveis pela gestão do contrato e fiscalização dos serviços serão definidos em correspondências após assinatura do contrato

15.5. 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:

SPTrans
São Paulo Transporte S/A
Área Gestora: Superintendência de Tecnologia da Informação e Comunicação – DG/STI
Nome do Gestor: Sr. Maurício Lima Ferreira
e-mail: mauricio.lima@sptrans.com.br
Endereço: Rua Boa Vista, 236 – 6 º andar – Meio – Centro – SP – CEP: 01014-000

Nome do Fiscal Administrativo: Sr. Maurício de Moraes
e-mail: mauricio.moraes@sptrans.com.br
Endereço: Rua Boa Vista, 236 – 6 º andar – Centro – SP – CEP: 01014-000

Nome do Fiscal Técnico: Sr. Heitor Arantes Farres - DG/STI/GST
e-mail: heitor.farres@sptrans.com.br
Endereço: Rua Boa Vista, 236 – 6 º andar – Centro – SP – CEP: 01014-000

CONTRATADA
BRASTORAGE COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA. (THINK ABOUT IT)
Área Gestora: Divisão de Segurança
Nome do Gestor: Alexandre Noel de Azevedo
E-mail: Alexandre.azevedo@think.br.com
Endereço completo: Av. Maria Coelho do Aguiar, nº 215 – Bloco C – 3º andar CENESP – São Paulo – SP – CEP: 05804-900

15.6. 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.

15.7. Para as comunicações relativas à operacionalização do fornecimento do objeto do contrato, poderá ser utilizado correio eletrônico.

15.8. As substituições dos responsáveis de ambas as partes, bem como qualquer alteração dos seus dados, deverá ser imediatamente comunicada por escrito conforme o item 15.5 deste contrato.

15.9. Será competência do Gestor da **SPTrans**, dentre outras:

15.9.1. Provocar a instauração de processo administrativo com o objetivo de apurar responsabilidade ou prejuízo resultante de erro ou vício na execução do contrato ou de promover alteração contratual, especialmente no caso de solução adotada em projeto inadequado, desatualizado tecnologicamente ou inapropriado ao local específico;

15.9.2. Identificar a necessidade de modificar ou adequar a forma de execução do objeto contratado;

15.9.3. Acompanhar, durante toda a execução do contrato, com apoio do fiscal administrativo, a manutenção, pela **CONTRATADA**, de todas as condições de habilitação exigidas na licitação, em especial com relação à regularidade fiscal;

15.9.4. Atestar a plena execução do objeto contratado.

15.10. Serão deveres do representante ou preposto da **CONTRATADA**, dentre outros:

15.10.1. Zelar pela manutenção, durante todo o período de execução do contrato, das condições estabelecidas neste instrumento e das Normas Regulamentadoras e Legislação correlata do Meio Ambiente e Segurança e Medicina do Trabalho, como também da regularidade fiscal e obrigações trabalhistas;

15.10.2. Zelar pela execução ou fornecimento do objeto contratual em conformidade com as normas técnicas vigentes e manuais da **SPTrans**;

15.10.3. Zelar pela plena, total e perfeita execução do objeto contratado.

CLÁUSULA DÉCIMA SEXTA - 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 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- DA PROPRIEDADE, DIREITOS AUTORIAIS E CONFIDENCIALIDADE

17.1. A **SPTrans**, a partir da assinatura do contrato, será cessionária de direito de uso de toda informação contida em documentos técnicos, programas de computador e outros documentos relativos à execução do presente contrato, não se limitando, mas incluindo quaisquer documentos elaborados pela **CONTRATADA** no cumprimento deste contrato, obrigando-se a mesma a entregá-los à **SPTrans** sempre que solicitado.

17.2. Todos os dados gerados e armazenados pelo sistema serão de propriedade exclusiva da **SPTrans**, obrigando-se a **CONTRATADA**, quando obtiver acesso a esses dados, documentos e informações privilegiadas, a manter sigilo e confidencialidade absolutos perante terceiros.

17.3. Em caso de dúvida acerca da confidencialidade de determinada Informação, a **CONTRATADA** deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito a tratá-la diferentemente pela **SPTrans**. De forma alguma se interpretará o silêncio da **SPTrans** como liberação do compromisso de manter o sigilo da Informação.

17.4. Todos os produtos de software, documentos parciais e/ou finais decorrentes dos serviços objeto deste contrato somente serão recebidos pela **SPTrans** quando encaminhados pelo representante da **CONTRATADA**, diretamente à área gestora do contrato.

17.5. Caso a **CONTRATADA** seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer Informações, notificará por escrito a **SPTrans** imediatamente ou em até 24 (vinte e quatro) horas na impossibilidade de execução acerca da referida intimação, de forma a permitir que a SPTrans possa optar entre recorrer a uma liminar ou outro recurso apropriado para impedir a revelação ou consentir, por escrito, com referida revelação.

17.6. A **SPTrans** poderá a qualquer tempo solicitar que a **CONTRATADA**:

17.6.1. Entregue imediatamente a **SPTrans** todas as Informações (e todas as cópias das mesmas e outros documentos e materiais que incorporem ou reflitam quaisquer Informações) fornecidas de acordo com esta Cláusula;

17.6.2. Destrua referidas Informações (e todas as cópias e outros documentos e materiais) e certifique da destruição, por escrito, a **SPTrans**.

CLÁUSULA DÉCIMA OITAVA – DAS CONDIÇÕES DE RECEBIMENTO

18.1. Executado o contrato, o seu objeto deverá ser recebido:

18.1.1. Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita da **CONTRATADA**;

18.1.2. Definitivamente, pelo Gestor do Contrato, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação ou vistoria que comprove a adequação do objeto aos termos contratuais, no prazo máximo de 90 (noventa) dias contado do recebimento provisório.

18.2. O recebimento provisório ou definitivo não excluirá a responsabilidade civil, principalmente quanto à solidez e segurança da obra ou do serviço, nem ético-profissional pela perfeita execução nos limites estabelecidos pelo Código Civil Brasileiro e pelo contrato.

18.3. Nos casos devidamente justificados, os prazos para recebimento provisório e definitivo poderão ser prorrogados mediante autorização da autoridade competente, formalizada através de Termo Aditivo, desde que celebrado anteriormente ao término da vigência contratual.

18.4. Na hipótese de rescisão do contrato, caberá ao responsável pela fiscalização atestar as parcelas adequadamente concluídas, recebendo provisória ou definitivamente, conforme o caso.

CLÁUSULA DÉCIMA-NONA - DO ENCERRAMENTO DO CONTRATO

19.1. Executados os serviços, 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 e da emissão do Termo de Recebimento Definitivo.

CLÁUSULA VIGÉSIMA - DOS CASOS OMISSOS

20.1. 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 PRIMEIRA – DISPOSIÇÕES FINAIS

21.1. 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.

21.2. 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 **SPTrans**.

21.3. Em cumprimento ao item 7 do Código de Conduta e Integridade da SPTrans, os canais de denúncias relativas 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 **SPTrans**
Rua Boa Vista, 236 - 1º andar (Protocolo)

CLÁUSULA VIGÉSIMA SEGUNDA - DO FORO

22.1. 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.

Tânia Cristina Bozetti R. da Silva
Resp. 101453-8

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, 12 de maio de 2022.

SÃO PAULO TRANSPORTE S/A
"SPTrans"

[redacted]

MAURÍCIO LIMA FERREIRA
Procurador

[redacted]

[redacted]

GEORGE WILLIAM GIDALI
Diretor de Gestão da Receita e Remuneração

[redacted]

BRASTORAGE COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA. (THINK ABOUT IT)
"CONTRATADA"

[redacted]

CONSTANTINO ILIADIS
Sócio

[redacted]

MARCO AURÉLIO LORENA DE MELLO
Sócio

[redacted]

Testemunhas:

[redacted]

1ª
Nome: Tânia Cristina Bozetti R. da Silva
CPF n.º [redacted]

[redacted]

2ª
Nome: João Francisco Piovesani
CPF n.º [redacted]

CONTRATO [redacted] na
Gerência de Contrata[redacted]as da
SÃO PAULO TR[redacted] em
12/05/2022 S[redacted]

Tânia Cristina Bozetti R. da Silva

ANEXO I

TERMO DE REFERÊNCIA

SPTrans

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

SPTrans

ESPECIFICAÇÃO DO OBJETO

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, VARREDURA DE VULNERABILIDADES, TESTES DE INTRUSÃO/PENETRAÇÃO E GERAÇÃO DE RELATÓRIOS

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 e suporte a implantação de boas práticas.

1. CONDIÇÕES GERAIS:

1.1. O objetivo principal desta contratação é aumentar o nível de Segurança da Informação da SPTRANS através:

1.1.1.1. Monitoramento e gerenciamento de segurança em relação a comportamentos que apresentem riscos ao ambiente da SPTRANS;

1.1.1.2. Avaliações periódicas de falhas e vulnerabilidades de maneira recorrente;

1.1.1.3. 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;

1.1.1.4. 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;

1.1.1.5. 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.

1.1.1.6. Prover serviço de monitoramento da Surface, Dark e Deep Web sobre a marca da SPTRANS

1.1.1.7. Prover serviço de segurança baseado em Edge computing WAF.

1.1.1.8. O 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

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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, em todos os sistemas informatizados da SPTRANS.

2. CARACTERÍSTICAS GERAIS

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

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. O serviço também comtemplará uma solução para varredura de vulnerabilidades, testes de intrusão, "phishing" testes como serviço – SaaS, Manutenção e Relatórios.

2.1.5. 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.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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 reflita 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 reflita sua gravidade. A pontuação numérica pode

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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 acidental 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 dedados 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

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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;

4.1.1. Banco de Dados
4.1.2. Dispositivos
4.1.3. Aplicação
4.1.4. Link
4.1.5. Servidores
4.1.6. Segurança da infraestrutura e banco de dados;

Os detalhes destes itens acima estão apresentados no anexo I.

4.2. Monitoramento externos, ambiente WEB.

4.2.1. Monitoramento de repositórios públicos (pastebin, github, etc.) visando detectar informações confidenciais e forma pública, como trechos de código fonte, logins e senhas etc;
4.2.2. Detecção de sites de phishing ou que personificam a marca da SPTRANS e tentativa de eliminação;
4.2.3. Monitoramento em todas as camadas da WEB (surface, deep e dark-web) para detecção de possíveis ameaças e/ou vazamentos;
4.2.4. Monitoramento de uso indevido ou fraudulento da marca;
4.2.5. Monitoramento de domínio similares para execução de fraude;
4.2.6. Monitoramento de aplicativos falsos e disponibilizados em lugares como

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

Google Play e Apple Store;

4.3. Monitoramento internos e testes.

4.3.1. Avaliações em endpoints com antivírus da SPTRANS medindo a segurança;
4.3.2. Avaliação da segurança em redes e Wifi;
4.3.3. Varredura automática de ativos;
4.3.4. Scanner de vulnerabilidades Web (DAST), deverá ter dashboard de acompanhamento e comparativo da evolução da segurança, permitir a análise e re-execuções por demanda.
4.3.5. Baseline e conformidade dos ativos (hardening);
4.3.6. Ataques físicos contra a infraestrutura da SPTRANS;
4.3.7. Ataques físicos de engenharia social na infraestrutura da SPTRANS;
4.3.8. Analisar, 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;
4.3.9. Investigação forense, 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;
4.3.10. Realizar respostas aos incidentes cibernéticos decorrentes de vulnerabilidades sistêmicas;
4.3.11. Vigilância de meios de comunicação e análise de dados dos crackers e fraudadores;
4.3.12. Realizar a comunicação com outros CSIRT's, órgãos como CERT.br, CTIR, NIC, USCERT, entre outros, quando necessário;
4.3.13. Prover todos os alertas possíveis assim como recomendações para solução de falhas de "dia-zero"
4.3.14. Avaliação das políticas de backup;

4.4. Recursos internos

4.4.1. Para a prestação de serviço deverá prever 1 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.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Parí CEP 03026-030 – PABX 11 2796-3299

5. CARACTERÍSTICAS DO SERVIÇO DO SIEM

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

5.2. Arquitetura Básica

5.2.1. 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.

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

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

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

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

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

5.2.7. 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;

5.2.8. A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar os ativos descritos no anexo 1, que deverá ser apresentado o volume de EPS que a solução irá suportar;

5.2.9. 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.

5.2.10. 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;

5.2.11. 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;

5.2.12. Qualquer acesso deve ser feito de forma segura;

5.2.13. Ter suporte a monitoração a partir SNMPv2c ou versões posteriores.

5.2.14. A solução deve prover aceleradores de implementação, boas práticas e aumento da inteligência e funcionalidades através de integrações adicionais

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

e aplicações de terceiros, em formato de plug-in ou "App".

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

5.2.16. 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.

5.3. Processamento Interno nas dependências da SPTRANS

5.3.1. 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.

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

5.4. Tratamento de eventos

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

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

5.4.3. 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.

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

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

5.4.6. Gerar alertas/incidentes com base nas regras definidas previamente;

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

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

5.4.9. 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;

5.4.10. 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;

5.4.11. Permitir a visualização para a equipe do SOC do prestador, na

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

interface da aplicação, dos eventos relacionados a um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução;

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

5.4.13. 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;

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

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

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

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

5.4.18. 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.

5.4.19. 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.

5.4.20. 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.

5.5. Coleta de logs

5.5.1. 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;

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

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

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

5.5.5. Deverá fazer a agregação de eventos, mostrando a contagem de eventos,

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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;

5.5.6. Deve manter o evento bruto ("raw") e seus metadados para o armazenamento e consulta futura;

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

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

5.5.9. 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.

5.5.10. 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.

5.5.11. 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);

5.5.12. 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

5.5.13. 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.

5.6. A solução de Siem quanto ao Correlacionamento

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

5.6.2. Efetuar o correlacionamento dos eventos próximo ao tempo real;

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

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

5.6.5. 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;

5.6.6. 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;

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274. Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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

5.6.8. 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;

5.6.9. 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);

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

5.6.11. Integrar com ferramentas externas de diagnostico padrão tais como: Nslookup, Whois, Nmap;

5.6.12. 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;

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

5.6.14. 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;

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

5.6.16. Possuir pelo menos os seguintes tipos de correlação:

5.6.17. Correlação por regras;

5.6.18. Correlação por anomalia e padrão de comportamento;

5.6.19. 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);

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

5.6.21. 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;

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

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

5.6.24. Deve permitir usar as regras de correlação aplicada de forma histórica, em eventos já mantidos na base de dados da solução, sem afetar a

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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.

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

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

5.6.27. 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.

5.6.28. 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;

5.6.29. 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:

5.6.30. 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;

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

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

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

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

5.6.35. Detecção de ações relacionadas à mineração de moedas digitais;

5.6.36. 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;

5.7. Armazenamento de dados

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

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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

5.7.3. Deve armazenar os eventos em formato original ("raw") em conjunto com propriedades normalizadas e outros metadados, de forma a permitir a pesquisa e visualização;

5.7.4. Armazenar logs por tempo determinado e customizado;

5.7.5. 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;

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

5.7.7. 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;

5.7.8. 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;

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

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

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

5.7.12. 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.

5.7.13. 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.

5.7.14. 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.

5.8. Gerenciamento e Operação

5.8.1. Possuir acesso controlado e autenticado por usuário;

5.8.2. Possuir acesso seguro e criptografado à interface web, de forma a garantir a

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

confidencialidade;

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

5.8.4. 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;

5.8.5. 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;

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

5.8.7. 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.

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

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

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

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

5.8.12. 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;

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

5.8.14. 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;

5.8.15. 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;

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

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

5.8.18. 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;

5.8.19. Deve disponibilizar APIs do tipo webservices, do tipo "RESTful API", para acesso externo e integração com a solução, permitindo busca de

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274. Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pan CEP 03026-030 – PABX 11 2796-3299

informações de eventos e flows, manipulação de incidentes e uso de administração da solução;

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

5.8.21. 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;

5.9. Tratamento de Incidentes

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

5.9.2. Permitir associar os incidentes aos usuários da solução;

5.9.3. Permitir encerrar um incidente quando este for solucionado;

5.9.4. Permitir adicionar anotações aos incidentes para registro das ações tomadas ou observações;

5.9.5. 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;

5.9.6. Deve possuir integração suportada na solução, com ferramenta especializada no tratamento de resposta à incidente;

5.9.7. 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.

5.10. Compatibilidade e escalabilidade

5.10.1. A solução deverá executar sobre ambiente virtual, vmware e ou hyper-V.

5.10.2. 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);

5.10.3. A solução deve ter a capacidade para suportar a adição de novos componentes para garantir a escalabilidade, inclusive referente ao banco de dados;

5.10.4. 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 SPTrans ou seus fornecedores de serviço.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

5.10.5. Firewall

5.10.5.1. Checkpoint;
5.10.5.2. Cisco ASA;
5.10.5.3. Cisco FirePower;
5.10.5.4. Fortinet Fortigate;
5.10.5.5. Palo Alto Networks;
5.10.5.6. IPTables;
5.10.5.7. Watchgard

5.10.6. Detecção/Prevenção de Intrusos/Anti-DDoS

5.10.6.1. Sourcefire Defense Center;
5.10.6.2. Snort;
5.10.6.3. Cisco IPS;
5.10.6.4. Radware DefensePro;

5.10.7. Antivírus/Antimalware

5.10.7.1. Trend Micro;
5.10.7.2. Symantec System Center;
5.10.7.3. Symantec Endpoint Protection;
5.10.7.4. McAfee ePolicy Orchestrator (ePO);
5.10.7.5. Kaspersky Security Center;
5.10.7.6. FireEye;
5.10.7.7. F-secure

5.10.8. Sistemas Operacionais

5.10.8.1. Linux;
5.10.8.2. Microsoft Windows;

5.10.9. Servidor Web e Proxy

5.10.9.1. Microsoft IIS;
5.10.9.2. Apache;
5.10.9.3. NGinX Proxy Reverso;
5.10.9.4. Squid Web Proxy;
5.10.9.5. Websense

5.10.10. Roteadores/switches

5.10.10.1. 3com;

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

5.10.10.2. Nortel;
5.10.10.3. Extreme;
5.10.10.4. Enterasys;
5.10.10.5. Cisco;
5.10.10.6. Juniper;
5.10.10.7. Aruba;

5.10.11. Servidor de Banco de dados e Ferramentas de DAM

5.10.11.1. Oracle;
5.10.11.2. Microsoft SQL;

5.10.12. Scanners de vulnerabilidades

5.10.12.1. Nessus;
5.10.12.2. QualysQuard;
5.10.12.3. Foundstone;
5.10.12.4. NMAP;

5.10.13. Concentrador VPN;

5.10.13.1. NORTEL;
5.10.13.2. Check point UTM;
5.10.13.3. Cisco;

5.11. Relatórios

5.12. Comportamento de usuário.

5.12.1. 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).

5.12.2. 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.

5.12.3. 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.

5.12.4. 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.

5.12.5. Deve permitir selecionar usuários que não devem fazer parte da

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

análise com modelos de Machine Learning

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

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

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

5.12.9. 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

5.12.10. 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.

5.12.11. 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

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

5.12.13. Tentativa de acesso a contas suspensas;

5.12.14. Acesso negado repetido;

5.12.15. Usuário acessando a VPN a partir de uma localidade atípica;

5.12.16. Usuário acessando a VPN a partir de horários atípicos;

5.12.17. Conta utilizada numa quantidade atípica de atividades;

5.12.18. Acesso a máquinas Linux e Windows com contas de serviço;

5.12.19. Primeiro uso de um recurso importante por um usuário;

5.12.20. Acesso a endereços considerados suspeitos por bases de Threat feed/IP Reputation

5.12.21. Detecção de comandos em blacklist por um usuário

5.12.22. Conta de usuário criada em deletada rapidamente

5.12.23. Detecção de ataque de negação de serviço pela deleção de contas

5.12.24. Conta anômala criada a partir de uma nova localização

5.12.25. Conta anômala em Cloud, criada a partir de uma nova localização

5.12.26. Detecção de comportamento de Ransomware

5.12.27. Compliance para General Data Protection Regulation (GDPR) ou Lei Geral de Proteção a Dados (LGPD)

5.12.28. Deve ser capaz de aprender de forma supervisionada ou não supervisionada os comportamentos dos usuários;

5.12.29. Uso de LDAP/AD para análises de definição de grupos de usuários que deverão ser analisados como "Peer Groups" por algoritmos de machine learning

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

6. SOLUÇÃO PARA VARREDURA DE VULNERABILIDADES

6.1. 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.

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

6.3. 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.

6.4. 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.

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

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

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

6.8. 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;

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

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

7. CARACTERÍSTICAS TÉCNICAS PARA SOLUÇÃO VARREDURA DE VULNERABILIDADES

7.1. Todo o tráfego de informações entre a Solução e a Internet deve ser criptografado;

7.2. Todo o tráfego de informações entre o Gerenciador e os scanners deve ser criptografado.

7.3. Todos os scanners devem ser administrados por um Gerenciador único.

7.4. A solução deve possuir capacidade de receber atualizações em horários programados.

7.5. A solução deve suportar vários scanners conectados simultaneamente. Deverá a

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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.

7.6. A solução deve possuir capacidade de atualizar os scanners automaticamente.

7.7. A solução deve receber a atualização automática da base de vulnerabilidades.

7.8. A solução deve possuir uma base de vulnerabilidades fornecida pelo fabricante, que deve ser atualizada de forma incremental diretamente do site do fabricante.

7.9. A solução deve possuir uma base de análises que permite identificar vulnerabilidades CVE.

7.10. 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.

7.11. Se necessário, o scanner da solução deve funcionar sem necessidade de acesso à internet

7.12. 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.

7.13. A solução deve prover interface gráfica WEB para gerenciamento de todos os seus componentes e suas configurações.

7.14. A solução deve possuir suporte ao IP (Internet Protocol) versão 4 e versão 6.

8. REQUISITOS TÉCNICOS DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES

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

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

8.3. 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.

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

8.5. 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.

8.6. A solução deverá ter capacidade de realizar automaticamente (através de

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274. Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

agendamento automático) a descoberta de ativos;

8.7. 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.

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

8.9. 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.

8.10. Suportar efetuar varredura à procura de vulnerabilidades e exploits.

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

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

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

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

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

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

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

8.18. O Gerenciador deve possibilitar a configuração de desempenho na varredura de vulnerabilidades, como por número de conexões simultâneas e ativos simultâneos.

8.19. 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.

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

8.21. 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.

8.22. 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.

8.23. 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.

8.24. A ferramenta deve permitir escaneamentos específicos, utilizando no mínimo

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

os seguintes grupos de auditoria:

8.24.1. Deve possuir templates para varredura de vulnerabilidades mobile

8.24.2. Deve possuir templates para varredura de vulnerabilidades web application

8.24.3. Deve possuir templates para varredura de vulnerabilidades patch audit

8.24.4. Deve possuir templates para varredura de vulnerabilidades de acordo CIS

8.24.5. Deve possuir templates para varredura de vulnerabilidades de acordo PCI

8.24.6. Deve possuir condição de criação de modelos específicos com base no levantamento automatizada.

8.25. A solução de SIEM adotada deverá apontar os patchs necessários, com possibilidade de correlacionar as informações pela própria interface da ferramenta de gerenciamento de vulnerabilidades.

8.26. 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.

8.27. 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.

8.28. A solução deve prover modelo de validação de conformidade para a Norma PCI DSS.

8.29. A solução deve ser capaz de criar internos tickets para tratamento de vulnerabilidades, e distribuir estes para os usuários da Solução.

8.30. A solução deve ser capaz de enviar e-mails para criação de tickets externos para tratamento de vulnerabilidades em ferramentas de ITSM externas.

8.31. A solução deve der compatível pelo menos com os seguintes sistemas operacionais:

8.31.1. Windows Server 2008 SP2 ou maior (32-bits e 64-bits)

8.31.2. Windows 7 (32-bits e 64-bits)

8.31.3. Windows Server 2008 R2 SP1 ou maior (64-bits)

8.31.4. Windows 8 (32-bits e 64-bits)

8.31.5. Windows Server 2012 (64-bits)

8.31.6. Windows 8.1 (32-bits e 64-bits)

8.31.7. Windows 10 (32-bits e 64-bits)

8.31.8. Windows Server 2012 R2 (64-bits)

8.31.9. Windows Server 2016 (64-bits)

8.31.10. Linux

8.31.11. MacOS

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

9. TESTE DE INTRUSÃO/PENETRAÇÃO

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

9.1.1. 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;

9.1.2. 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;

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

9.2. O Teste de Negação de Serviço (DooS) 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.

9.3. Teste de Penetração Interno.

9.3.1. A CONTRATADA deverá realizar pelo 1 teste intrusão 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.

9.4. Teste de Penetração Externo.

9.4.1. 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 os principais aplicações e sistemas críticos.

9.5. 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.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274 Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

9.6. 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.

9.7. 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.

9.8. Deverão ser testados, minimamente, os seguintes quesitos, quando pertinentes:

9.8.1. Validação de acesso lógico
9.8.2. Segmentos de rede
9.8.3. VLANs
9.8.4. Burlar regras de firewall
9.8.5. Obtenção de informações
9.8.6. Enumeração de usuários
9.8.7. Sniffing
9.8.8. ARP Spoofing
9.8.9. Segurança dos dados
9.8.10. Canal de comunicação
9.8.11. Cifras fracas
9.8.12. Armazenamento inseguro
9.8.13. Descoberta de Senhas
9.8.14. Força bruta
9.8.15. Ataque off-line
9.8.16. Arquitetura da rede
9.8.17. Acesso remoto e VPN
9.8.18. Protocolos de comunicação
9.8.19. Mixed Content/Scripting;
9.8.20. Unvalidated Redirects;
9.8.21. Insecure Cookies;
9.8.22. Iframe Injection;
9.8.23. Clickjacking;
9.8.24. Cross Site Scripting (XSS);
9.8.25. Cross Site Request Forgery (XSRF);
9.8.26. Cross Site Script Inclusion (XSSI);
9.8.27. HTTP Parameter Pollution;

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

9.8.28. Path Traversal;
9.8.29. Buffer Overflow;
9.8.30. Integer Overflow;
9.8.31. Privilege Escalation;
9.8.32. Authentication Bypass;
9.8.33. Information Leak;
9.8.34. Local File Inclusion;
9.8.35. Remote File Inclusion;
9.8.36. Source Code Disclosure;
9.8.37. SQL Injection;
9.8.38. Remote Code Execution;
9.8.39. Revisão das vulnerabilidades listadas no OWASP Top 10
9.8.40. Insecure Direct Object Reference.

9.9. 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.

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

9.11. 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;

9.12. 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.

9.13. 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.

9.14. 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;

9.15. 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.

9.16. Deverá a CONTRATADA realizar os testes de intrusão/penetração externos, de forma a explorar possíveis vulnerabilidades nos serviços disponíveis.

9.17. 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.

9.18. 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 na Tabela 1 e definida pela CONTRATANTE.

9.19. 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.

9.20. 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;

9.21. Os Testes de Intrusão poderão ser direcionados aos servidores Web e respectivas aplicações do serviço de hospedagem contratado pela CONTRATANTE.

9.22. 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.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

10. TESTES DE INVASÃO EM APLICAÇÕES WEB CONTINUO E RECORRENTE

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

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

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

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

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

10.6. 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.

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

10.8. Deverão ser analisadas, pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.

10.9. Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações.

11. SOLUCÃO WEB APPLICATION FIREWALL (WAF)

11.1. 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, garantindo o isolamento antes de impactar a infraestrutura da SPTRANS.

11.2. Deverá permitir a geração de log de eventos para análise e revisão de regras para a decisão de bloqueio e ajuste.

11.3. 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.

11.4. 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.

11.5. 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.

11.6. O produto de CDN (content delivery network) associado ao WAF a ser contratado deverá conter pelo menos 03 plataformas de tráfego de conteúdo

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

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.

12. CONDIÇÕES PARA EXECUÇÃO DO TRABALHO

12.1. Deverá a CONTRATADA obedecer a cronologia e ordenar o nível de criticidade de vulnerabilidades detectadas durante as varreduras, para geração de relatórios;

12.2. 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.

12.3. 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;

12.4. 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.

12.5. A CONTRATADA deverá revisar acessos e credenciais administrativas do ambiente de firewall atual, informando sobre melhorias necessárias.

12.6. 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.

12.7. 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.

13. QUALIFICAÇÃO TÉCNICA EXIGIDA DOS PROFISSIONAIS DA CONTRATADA

13.1. A seguir são definidos os requisitos mínimos obrigatórios e necessários, por categoria de serviço, para os perfis profissionais a serem alocados na execução contratual, conforme estabelecido nos itens relativos ao objeto dos serviços a serem contratados.

13.2. Empresa com no mínimo 10 anos de experiência no segmento de tecnologia com clientes de missão crítica.

13.3. Experiência e parceria com fabricantes de equipamentos, sistemas

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

operacionais e principais bancos de dados a fim de garantir acesso a informações, suporte e conhecimento de segurança apropriado.

13.4. Ter referências do mercado em clientes nacionais, capacidade de suportar operações em regime 24 x 7 atestados por pelo menos 3 clientes.

13.5. Experiência comprovada em atuação de investigação criminal e análise forense em ambiente computacional, demonstração de expertise comprovada com referências nacionais.

13.6. Empresa que tenha comprovadamente mais de 400 mil eventos monitorados mensalmente em suas operações de NOC/SOC.

13.7. A CONTRATADA deverá apresentar certificações de especialista em Ethical Hacker:

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

14.1. 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;

14.2. 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;

14.3. 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 e/ou e-mail a ser definido;

15. NÍVEL DE SERVIÇOS

15.1. 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 ou roubo de informações em ambiente crítico.
Média	4 horas	8 horas	Medio Risco, impacto individual em um ambiente de baixo

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

			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	Indisponiblidade do SCAN no processo de execução.

16. SUPORTE TÉCNICO DA SOLUÇÃO DE VARREDURA DE VULNERABILIDADES.

16.1. Deverá a CONTRATADA prover todo o suporte técnico das soluções adotadas, desde o inicio da operação e em eventuais manutenções ou atualizações que as ferramentas utilizadas para a prestação do serviço venha sofrer obedecendo o tempo Nível de Serviços sem custo adicional a SPTRANS.

16.2. *A CONTRATADA de verá prover um Portal Web, telefone e/ou e-mail, para abertura dos* **chamados.**

17. PRODUÇÃO DE RELATÓRIOS

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

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

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

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

17.4.1. Sumário Executivo: Este relatório deve apresentar um resumo do ambiente atual.

17.4.2. 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

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

descoberta e uma lista de ativos afetados.

17.4.3. Vulnerabilidades excluídas: Este relatório exibe ativos que tiveram vulnerabilidades excluídas, incluindo a razão da exclusão.

17.4.4. Compliance de ativos mensal: Este relatório deve apresentar as tendências de conformidade de ativos em seus agrupamentos.

17.4.5. Scorecard de Vulnerabilidades: Este relatório deve detalhar a idade da gravidade da vulnerabilidade e contagem no scorecard.

17.4.6. Matriz de Riscos por Vulnerabilidades: Este relatório deve detalhar o risco pelo impacto CVSS agrupado pela contagem de vulnerabilidades.

17.4.7. Matriz de Riscos por Ativos: Este relatório deve detalhar o risco pelo impacto CVSS agrupado por ativos.

17.5. Integrações necessárias para solução de varredura de vulnerabilidades

17.5.1. A solução deverá possuir capacidade de integração com o serviço de diretório LDAP.

17.5.2. A solução deverá possuir capacidade de integração com o serviço de diretório Microsoft Active Directory.

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

17.5.4. Deverão ser entregues os relatórios em até 10(dez) dias corridos, após termino da atividade.

17.6. Manutenção da solução de varredura de vulnerabilidades

17.6.1. 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 mior transparência de esforço e responsabilidade.

17.6.2. 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;

17.6.3. Caberá à CONTRATADA notificar o CONTRATANTE caso haja alguma indisponibilidade *do serviço prestado.*

18. DO PRAZO

18.1 O prazo de vigência deste contrato será de até 180 (cento e oitenta) dias, a contar de sua assinatura.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

19. FORMA DE PAGAMENTO

19.1 Os pagamentos serão efetuados 30 (trinta) dias após a data de entrega e aceite das Notas Fiscais/Faturas, na "SPTRANS", por meio de crédito em conta corrente que a CONTRATADA deverá manter no banco a ser indicado pela "SPTRANS".

Anexo I - AMBIENTE A SER MONITORADO NO SOC

Escopo de volume de ativos para o processo de SIEM, SCAN e Penetration Test.

Descrição	Quantidade
AD/Auth, DHCP, DNS	10
Servidor de Web e Mail	2
Windows e Linux de uso geral	150
Antivírus, Anti-Malware	2
Servidores de banco de dados	20
Servidor Proxy e pequenos Firewalls de borda	8
Switch Core e Firewalls de alto volume	4
IDS, IPS, VPN, LB	4
Roteadores e Switches	60
URLS:\\Aplication	20

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista 274 Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

ANEXO II

TERMO DE CONFIDENCIALIDADE

PREGÃO ELETRÔNICO n.º ____/_____

Os abaixo assinados, de um lado ***NOME EMPRESA***, constituída e validamente existente de acordo com as leis da República Federativa do Brasil, sita à RUA, Nº, COMPLEMENTO, BAIRRO, CIDADE, inscrita no CNPJ sob o nº XXXXXXXXXXXXX, doravante designada "XXXXXX", e, de outro lado a SÃO Paulo Transporte S/A, sito à Rua 3 de Dezembro, 34 – Centro – CEP 01014-020 na cidade de São Paulo, Estado de São Paulo, inscrito no CNPJ sob o nº 60.498.417/0001-58, doravante designado como "SPTRANS", têm entre si certa e ajustada a celebração do presente Termo de Confidencialidade, que se regerá pelas seguintes cláusulas e condições:

Considerando que a XXXXXX e a SPTRANS desejam cooperar nos campos tecnológico e comercial e que, sob a elaboração de proposta técnico/comercial visando atender ao pregão e processo acima identificados, a NOME DA EMPRESA precisará necessariamente ter acesso, avaliar e analisar determinadas Informações relativas a SPTRANS, que são consideradas pelo mesmo como proprietárias e confidenciais, a NOME DA EMPRESA concorda desde já, neste ato, em tratar todas as Informações relativas a SPTRANS, que lhe foram fornecidas ou que ainda lhe serão, bem como aos seus Representantes, consoante este Termo e suas cláusulas mencionadas abaixo:

PRIMEIRA – INFORMAÇÕES - Conforme utilizada neste Termo, a expressão "Informações" inclui quaisquer informações reveladas antes ou depois da data deste Termo, acerca da SPTRANS, seus bens de informação, topologias, planos, processos, operações, pessoal, propriedades, clientes, produtos e serviços, que a SPTRANS considerar proprietárias e/ou confidenciais.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274, Mezanino, Centro, CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

PARÁGRAFO ÚNICO – Em caso de dúvida acerca da confidencialidade de determinada Informação, a NOME DA EMPRESA deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito a tratá-la diferentemente pela SPTRANS. De forma alguma se interpretará o silêncio da SPTRANS como liberação do compromisso de manter o sigilo da Informação.

SEGUNDA – EXCEÇÕES – Para os fins deste Termo, a expressão "Informações" não inclui informações ou materiais que a NOME DA EMPRESA evidencie:

a) já estarem disponíveis ao público em geral de qualquer forma que não em decorrência de sua revelação pela SPTRANS;

b) já estarem legalmente disponíveis à NOME DA EMPRESA antes de referidas informações ou materiais terem sido fornecidos pela SPTRANS, de acordo com este Termo.

TERCEIRA – REPRESENTANTES - Conforme utilizada neste Termo, a expressão "Representantes" inclui os diretores, administradores, acionistas, proprietários, sócios, empregados, agentes, colaboradores, representantes, assessores e prestadores de serviços a qualquer título (incluindo, sem limitações, advogados, contadores, consultores e assessores financeiros) da NOME DA EMPRESA.

QUARTA – UTILIZAÇÃO DAS INFORMAÇÕES – A NOME DA EMPRESA concorda que as informações serão utilizadas somente para a elaboração de proposta técnico/comercial visando atender ao pregão e processo identificados entre as partes. Ademais, concorda também em informar seus respectivos Representantes acerca da natureza confidencial das Informações e em fazer com que tais Representantes tratem referidas Informações como confidenciais, de acordo com este Termo.

PARÁGRAFO ÚNICO - As partes concordam em não revelar as cláusulas e condições deste Termo, bem como os negócios objeto das negociações entre as mesmas ou qualquer de seus elementos, sem o prévio consentimento escrito da outra parte.

QUINTA – EVENTUAL DISPENSA DA CONFIDENCIALIDADE - Caso a NOME DA EMPRESA (ou qualquer dos seus Representantes) seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer Informações, notificará por escrito a SPTRANS imediatamente ou em até 24 (vinte e quatro) horas na impossibilidade de execução acerca da referida intimação, de forma a permitir que a SPTRANS possa optar entre recorrer a uma liminar ou outro recurso apropriado para impedir a revelação ou consentir, por escrito, com referida revelação.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800 Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299
Rua Boa Vista, 274 Mezanino Centro CEP 01014-000

SEXTA - TÉRMINO DE RELAÇÕES NEGOCIAIS ENTRE AS PARTES – A SPTRANS poderá a qualquer tempo solicitar que a NOME DA EMPRESA:

a) entregue imediatamente a SPTRANS todas as Informações (e todas as cópias das mesmas e outros documentos e materiais que incorporem ou reflitam quaisquer Informações) fornecidas de acordo com este Termo; ou

b) destrua referidas Informações (e todas as cópias e outros documentos e materiais) e certifique da destruição, por escrito, a SPTRANS.

PARÁGRAFO ÚNICO - Sem prejuízo da devolução ou destruição das Informações, a NOME DA EMPRESA e seus respectivos Representantes permanecerão responsáveis por suas respectivas obrigações de confidencialidade e demais obrigações assumidas sob este Termo, por um prazo de 20 (vinte) anos a contar da data do término das negociações entre as partes.

SÉTIMA – LIMITES - Este Termo não obriga qualquer das partes a iniciar negociações, discussões ou outras atividades relativas a quaisquer oportunidades de negócios, acordos ou contratos com a outra parte. A decisão de iniciar referidas atividades será tomada por cada uma das partes, a seu exclusivo critério.

OITAVA – VIGÊNCIA - As obrigações estabelecidas neste Termo vigorarão por um prazo de 20 (vinte) anos, contados da data deste Termo. Qualquer contrato ou acordo escrito entre as partes no tocante à negociação ora contemplada prevalecerá sobre este Termo e regerá as obrigações de confidencialidade das partes no tocante a quaisquer Informações relativas à negociação, sendo certo, porém, que este Termo permanecerá em pleno vigor e efeito para quaisquer outras Informações regidas sob este Termo.

NONA – FORO - Para dirimir as questões resultantes da execução do presente Termo de Confidencialidade, as partes elegem o foro da comarca de São Paulo - SP, com expressa renúncia de qualquer outro, por mais privilegiado que possa ser. Poderá, todavia, qualquer das partes optar, em caso de litígio, pelo foro do domicílio da outra parte.

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800 Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

E assim, por estarem justas e acordadas, assinam as partes este instrumento em 02 (duas) vias de igual teor e para um só efeito, na presença das testemunhas abaixo.

São Paulo, xx de Abril de 2022.

NOME DA EMPRESA

Nome: XXXXXXXXXX
Cargo: XXXXXXXXXX
E-mail: XXXXXXXXXX
Tel. XXXXXXXXXX; Cel: XXXXXX

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Boa Vista, 274 Mezanino Centro CEP 01014-000
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

ANEXO III

PLANILHA DE QUANTIDADES E PREÇOS

DESCRIÇÃO SERVIÇOS	UNIDADE DE MENSURAÇÃO	QUANTIDADE ITENS	VALOR UNITÁRIO	VALOR TOTAL
SOC MONITORAMENTO 24 X 7 SOC/SIEM	EPS	TODOS ANEXO1		
SOC SCAN VULNERABILIDADE	VOLUME DE ATIVOS	280		
PROTEÇÃO AVANÇADA ZERODAY SYSCAL LINUX	VOLUME DE HOST LINUX	150		
TESTE DE PENETRAÇÂO	QUANTIDADE	1		
MONITORAMENTO MARCA SPTRANS	VOLUME DE MARCA	1		
WAF	VOLUME DE APLICAÇÕES	20		

São Paulo Transporte S/A
End. Corresp. Rua Boa Vista, 236 Centro CEP 01014-000 PABX 11 3396-6800
Rua Santa Rita, 500 Pari CEP 03026-030 – PABX 11 2796-3299

ANEXO II

PROPOSTA COMERCIAL

think
MANAGED SERVICE PROVIDER

Proposta

SPTrans

Contratação de serviços gerenciados de segurança da informação.

DATA DE EMISSÃO: 19.04.2022

DATA DA REVISÃO: 19.04.2022

Proposta: 2836599308.2022-1

Responsável técnico: Marcos Pires

Responsável comercial: Alexandre Azevedo

Carta de agradecimento

A equipe **THINK IT** sente-se honrada pelo convite da **SPTrans** em participar da oferta de prestação de serviços de Segurança da Informação.

Somos especialistas em soluções de infraestrutura e segurança de TI, nosso time técnico e comercial é composto de profissionais altamente especializados e certificados, com experiência profissional de mais de 20 anos em ambientes de missão crítica (monitoração, operação e suporte de infraestrutura TI e Segurança da Informação), garantindo assim, o alcance dos objetivos estabelecidos de forma eficiente e eficaz, conforme abordagem detalhada na presente proposta de colaboração.

Sendo assim, estamos confiantes que a **THINK IT** possui todas as qualificações necessárias para atendê-los nesta importante iniciativa e esperamos, sinceramente, que o material aqui apresentado possa mostrar-lhes adequadamente nossos serviços e produtos. Agradecemos o interesse e nos colocamos à disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

Atenciosamente,

Alexandre Azevedo
Vice-Presidente Comercial
Think IT(Brastorage)

Índice

1 COMPROMISSO EXECUTIVO

A **THINK IT** declara pleno entendimento dos requerimentos da **SPTrans** para o 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**

Declara ainda seu compromisso com o atendimento dos objetivos apresentados.

Há mais de 14 anos, atuamos na prestação dos serviços referenciados neste processo de seleção de fornecedores. Durante todo este tempo, não medimos esforços para atuar sob um modelo de estreita proximidade e de parceria com nossos clientes, visando sempre entender e atender às necessidades do negócio. Nossa constante busca pela excelência é refletida pelos elevados índices alcançados de satisfação dos nossos clientes.

Esperamos, ao final de todo este processo, não somente mostrar que somos capazes de atender aos novos requisitos solicitados, iremos trabalhar para elevar a patamares únicos no mercado, os níveis de qualidade que já entregamos com segurança, eficiência e governança à **SPTrans**.

Atenciosamente,

Alexandre Azevedo
Vice-Presidente Comercial

2 QUEM SOMOS

A **THINK IT** é uma empresa formada por executivos com mais de 20 anos de experiência no mercado de prestação de serviços de infraestrutura de TI. Há 14 anos, foi fundada para preencher uma grande lacuna neste segmento: *ser uma empresa que entrega* ***excelência no gerenciamento*** *de serviços e ambientes de infraestrutura de TI com capacidade e flexibilidade para entender e atender às* ***necessidades de negócio dos nossos clientes.***

Entendemos que os **Serviços Técnicos Especializados de Segurança da Informação** não podem ser tratado como "commodity", pois cada cliente tem suas particularidades. A capacidade de entender estas particularidades, oferecendo um serviço com forte componente "***tailor made***", alinhado às necessidades do negócio, entregando excelência, tem sido a base do sucesso da **THINK IT** neste mercado tão competitivo.

Somos uma empresa de **soluções** que atua em toda a cadeia de serviços na área de infraestrutura de TI.

A figura a seguir relata, de forma sucinta, os principais produtos que compõem o nosso portfólio. Esses produtos foram pensados e estruturados de forma a facilitar a composição das soluções ofertadas, agregando **Segurança**, **flexibilidade**, **velocidade** e **qualidade** de entrega aos nossos clientes.

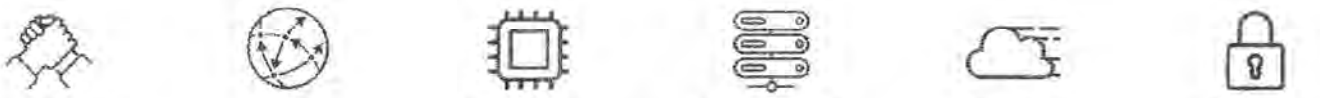


Figura 2 – Nossos produtos

Este modelo de atuação fez da **THINK IT** uma empresa de sucesso. Nosso faturamento cresceu mais de 5 vezes nos últimos 5 anos. Hoje temos mais de 180 clientes ativos e gerenciamos ativos de infraestrutura de TI que suportam um faturamento de mais de R$ 200 bilhões/ano, distribuídos pelos mais variados setores da economia. Conquistamos

vários prêmios internacionais por entregar soluções que resolveram, de forma inovadora, grandes problemas relacionados ao negócio. Temos elevado índice de satisfação e reconhecimento por parte de todos os nossos clientes.

A figura abaixo relata, de forma sucinta, os principais acontecimentos destes 14 anos de história.

Figura 3 – Nossa trajetória

2.1 SOBRE A THINK IT

Somos uma empresa MSP – ***Managed Service Provider*** de TI.

Nosso principal objetivo é ajudar nossos clientes a atingir seus desafios de negócio, aliando **conhecimento**, **talento** e rigor metodológico para a otimização, garantia de segurança e eficiência de ambientes de infraestrutura de TI.

De forma **segura**, **inovadora**, **comprometida, dinâmica** e **flexível**, colaboramos com nossos clientes, atuando em toda a cadeia de valor de infraestrutura de TI, desenvolvendo soluções e parcerias de longo prazo.

3 VISÃO GERAL

A partir da solicitação, por meio do Termo de Referência recebido pela nossa empresa, a **THINK IT** entende que a **SPTrans** busca um parceiro especializado em serviços de segurança da informação para fornecimento do seguinte resumo descritivo conforme o OBJETO descrito abaixo:

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 e suporte a implantação de boas práticas.

4 OBJETIVO

O objetivo principal desta contratação é aumentar o nível de Segurança da Informação da SPTrans.

5 NOSSA SOLUÇÃO

A solução está composta por um conjunto de serviços e tecnologias para atender todos os serviços descritos na TR, nossos serviços foram divididos em 3 grandes grupos:

Serviços de Técnicos Especializados

1. Penetration Test
2. Monitoramento da Marca SPTrans

Ferramentas de apoio

1. Ferramenta para Detecção de Explorações Avançadas
2. Scan de Vulnerabilidade

Serviços 24x7 de monitoramento e gestão de segurança da informação (SOC).

3. SOC
4. WAF

6 DESCRIÇÃO DE SERVIÇOS

Neste capítulo detalhamos nossos serviços a **SPTrans**.

Faz parte do escopo dessa proposta a detecção de falhas e vulnerabilidades de segurança da informação nos sistemas do cliente, por meio dos seguintes serviços:

6.1 PENETRATION TEST

- Será executado com equipe de Cyber Army e ferramentas de inteligência artificial no site e na infraestrutura que o suporta (sistemas operacionais, web servers, application servers, servidores de banco de dados, entre outros), para elaboração de relatórios e posterior correção das fragilidades detectadas;
- Serviços Técnicos Especializados para solução das vulnerabilidades detectadas (incluindo retestes ilimitados);
- Serviços Técnicos Especializados para implementação das melhores práticas de segurança da informação;
- Serviços Técnicos Especializados no direcionamento da equipe da SPTtrans no desenvolvimento seguro de novas aplicações;
- ALVOS PARA OS TESTES DE SEGURANÇA DA INFORMAÇÃO
- Disponível em: https://*SPTRANS.com.br*/

6.1.1 FORA DO ESCOPO

Não fazem parte do escopo dessa proposta:

- Detecção ou análise de falhas e vulnerabilidades em quaisquer outros sistemas de TI que não façam parte de ou que não estejam eletronicamente conectados aos sistemas descritos nessa proposta;
- Ataques físicos contra a infraestrutura do cliente ou de terceiros;
- Ataques de engenharia social contra colaboradores e fornecedores do cliente.

6.1.2 MÉTODO

Nosso método de trabalho compreende as seguintes etapas:

- Reunião de lançamento do projeto (*kick-off*):

Apresentação dos objetivos do projeto, definição do *modus operandi*, estabelecimento das equipes de trabalho, incluindo papéis, responsabilidades, autorizações e recursos necessários.

- Identificação dos alvos da análise:

Listagem dos diferentes alvos da análise, como aplicações Web, domínios, subdomínios, endereços IP e demais serviços associados.

- Coleta e análise de informações do ambiente das aplicações:

Levantamento detalhado das informações relacionadas aos elementos da arquitetura das aplicações e interfaces, como sistemas operacionais, linguagens de programação, serviços, *software*, *firewalls*, *webservices*, tipos de servidores e *plug-ins*.

- Pesquisa e análise de vulnerabilidades das aplicações:

Realização de teste de invasão externo "cego" (*black-box penetration test*) ou teste de invasão semi-orientado (*grey-box penetration test*), visando a identificação de falhas de segurança e a exploração em profundidade das mesmas. Também envolve a detecção de *malware*, localizando possíveis páginas ou serviços já infectados por algum código malicioso.

- Diagnóstico das fragilidades tecnológicas:

Elaboração de relatórios técnicos intermediários, contendo riscos identificados, evidências, profundidade das vulnerabilidades, recomendações de soluções correlatas e consolidação das informações dos resultados obtidos. As vulnerabilidades apontadas serão classificadas conforme o risco: Informacional, Baixo, Médio, Alto e Crítico.

- Reuniões intermediárias de equipes técnicas:

- Apresentação de relatórios técnicos, esclarecimento de dúvidas das equipes técnicas do cliente, suporte à tomada de decisões quanto à mitigação dos riscos e solução das falhas e vulnerabilidades encontradas. Pode ser presencial ou remota.

- Validação das correções de falhas e vulnerabilidades:

Caso o cliente implemente soluções para mitigação dos riscos, a equipe técnica da Think IT Security fará a validação das correções, durante um prazo máximo de 90 (noventa) dias, e emitirá um relatório sobre a eficácia das mesmas.

- Reunião de encerramento do projeto:

Apresentação final do trabalho realizado, relatórios técnicos correlatos e suas conclusões, bem como sugestões ao cliente.

6.1.3 ENTREGÁVEIS

Serão entregues, com base nos resultados obtidos com a prestação de serviços aqui ofertados pela *THINK IT*, em idioma português, no formato eletrônico PDF ou Microsoft Office, os seguintes documentos:

1. **Relatório Parcial de Falhas e Vulnerabilidades de Segurança da Informação:**
   Entregue quinzenalmente, contendo a relação de falhas e vulnerabilidades nos sistemas-alvos identificadas durante o respectivo período, bem como uma avaliação da criticidade das mesmas e sugestão de ações para eliminação, quando for o caso. O procedimento de envio deste tipo de relatório será definido em comum acordo.
2. **Relatório Extraordinário de Falhas e Vulnerabilidades Graves e Críticas de Segurança da Informação:**
   Entregue assim que uma falha ou vulnerabilidade classificada como de Risco Alto ou Crítico tenha sido identificada. O procedimento de envio deste tipo de relatório será definido em comum acordo entre as partes.
3. **Relatório de Estado de Desenvolvimento dos Serviços:**
   Entregue mensalmente, consolida todas as atividades e resultados obtidos durante

o período, destacando questões relevantes, pontos de atenção que demandem ações por parte da equipe do cliente e consumo de recursos.

4. **Base de Dados de Falhas e Vulnerabilidades de Segurança da Informação:** Planilha eletrônica ou plataforma WEB, atualizada quinzenalmente até o encerramento dos serviços prestados, contendo a identificação de falhas e vulnerabilidades de segurança da informação encontradas, nível de criticidade do risco, descrição do método de teste e demais informações técnicas associadas, visando dar suporte às atividades de diagnóstico e correção a serem executadas pelos profissionais do cliente, como páginas Web, serviços, sistemas computacionais, vias de acesso e procedimentos de teste, quando disponíveis.

6.1.4 CARACTERÍSTICAS DOS TESTES

Para identificação dos riscos de segurança relacionados a falhas e vulnerabilidades, são utilizadas duas abordagens de teste: manual e automática.

Os testes manuais realizados pelos profissionais da equipe técnica da Think IT Security envolvem a análise individual de todas as páginas Web, serviços e requisições do sistema do cliente, repetida por múltiplas vezes e por no mínimo uma dupla de engenheiros, seguindo métodos próprios e exclusivos da THINK IT, de amplo espectro (*client-side* e *server-side*). Durante todos os testes manuais, nossos engenheiros trabalham sempre em duplas, otimizando os serviços e aumentando sua qualidade.

Dentre todas as vulnerabilidades testadas manualmente, seguem alguns exemplos:

Já os testes automáticos são realizados com as melhores ferramentas de mercado e com nossa ferramenta exclusiva. Ela é uma ferramenta de altíssima precisão e performance, baseada em inteligência artificial, que "aprende" com o sistema testado e agrega automação ao trabalho de um especialista de segurança, detectando falhas complexas e de lógica difusa. Ela grava requisições legítimas executadas por um operador, como transações bancárias e alterações de cadastro pessoal. E com base nessas requisições e em seus resultados, o operador define quais elementos da requisição são de

segurança quais elementos do resultado são confidenciais (dados pessoais) e quais elementos são esperados no retorno.

Quanto mais informações sobre a aplicação coletar, maior é a chance de detecção de possíveis falhas existentes. Uma vez obtidas essas informações, a ferramenta inicia testes exclusivos com o propósito de executar uma requisição ilegítima com sucesso, como:

- Validação de acesso lógico
- Segmentos de rede
- VLANs
- Burlar regras de firewall
- Obtenção de informações
- Enumeração de usuários
- Sniffing
- ARP Spoofing
- Segurança dos dados
- Canal de comunicação
- Cifras fracas
- Armazenamento inseguro
- Descoberta de Senhas
- Força bruta
- Ataque off-line
- Arquitetura da rede
- Acesso remoto e VPN
- Protocolos de comunicação
- Mixed Content/Scripting;
- Unvalidated Redirects;
- Insecure Cookies;
- Iframe Injection;
- Clickjacking;
- Cross Site Scripting (XSS);
- Cross Site Request Forgery (XSRF);

- Cross Site Script Inclusion (XSSI);
- HTTP Parameter Pollution;
- Path Traversal;
- Buffer Overflow;
- Integer Overflow;
- Privilege Escalation;
- Authentication Bypass;
- Information Leak;
- Local File Inclusion;
- Remote File Inclusion;
- Source Code Disclosure;
- SQL Injection;
- Remote Code Execution;
- Revisão das vulnerabilidades listadas no OWASP Top 10
- Insecure Direct Object Reference.

    - Acessar informações de outros usuários;
    - Executar uma operação sem utilizar elementos obrigatórios de segurança (senhas, *tokens*, entre outros);
    - Entre outras.

Além dos testes detalhados anteriormente, a ferramenta também busca por vulnerabilidades básicas, como SQL Injection e Cross Site Scripting, utilizando metodologia específica exclusiva, que diminui drasticamente falso-positivos e falso-negativos.

6.1.5 LOCAL DE TRABALHO

A realização das reuniões conjuntas entre os profissionais da THINK IT e do cliente se darão nas dependências do cliente ou por meio de serviço de comunicação remota.

A prestação de serviços se dará em locais externos às dependências do cliente.

6.2 MONITORAMENTO DA MARCA SPTrans

- 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;
- Declaramos o entendimento e atendimento de 100% dos itens 4.2 do Termo de Referência.

6.3 FERRAMENTA PARA DETECÇÃO DE EXPLORAÇÕES AVANÇADAS

Ferramenta para detecção de explorações avançadas – Advanced Persistent Threads (APTs). A ferramenta atua como um patch a nível de Kernel do sistema operacional, de forma a ser capaz de monitorar, em tempo real, todas as invocações a funções de sistema (syscalls) que possam ter relação com ações não autorizadas (ex.: execução de comandos por daemons, criação de sockets, abertura de arquivos, etc). Desta forma, é possível detectar o comprometimento de um sistema operacional de forma efetiva (a exemplo de vulnerabilidades de execução remota de código – RCE), mesmo nos casos em que os atacantes façam uso de ferramentas avançadas e falhas privadas (0 days) – visto que, a nível de Kernel, toda exploração, necessariamente, irá invocar syscalls (seja para executar comandos, criar ou ler arquivos, por exemplo). Uma vez detectada uma violação, o agente pode tomar uma ação imediata (ex.: colocar o servidor off-line) e envia alertas para os operadores do SOC – tendo em vista evitar um grande incidente de segurança desde o primeiro momento.

6.4 SCAN DE VULNERABILIDADES

A análise de vulnerabilidade ocorrerá sobre todos os ativos descritos no Anexo 1 do Termo de Referência.

6.4.1 TECNOLOGIA

Iremos trabalhar com uma combinaçãc de scanners ativos, agentes de monitoramento, para ajudar a maximizar a cobertura de verificação em toda a sua infraestrutura e reduzir os pontos cegos de vulnerabilidade. Essa combinação de tipos de sensores de dados ajuda a incluir ativos de difícil verificação no programa de gerenciamento de vulnerabilidades. Usamos algoritmo avançado de identificação de ativos, um extenso conjunto de atributos (como ID, nome do NetBIOS, enderecço MAC e muitos outros) para identificar e rastrear com precisão alterações em ativos, independentemente de como vagam ou de quanto tempo duram.

6.4.2 EFICIÊNCIA.

O nosso processo prioriza vulnerabilidades com base na probabilidade de serem utilizadas em um ataque por meio da combinação de mais de 150 fontes de dados, incluindo vulnerabilidades e dados de ameaças de terceiros. Um algoritmo proprietário de aprendizado de máquina e utilizado para identificar as vulnerabilidades com a maior probabilidade de ser exploradas para ajudar a se concentrar primeiro nos problemas de segurança mais importantes para a sua organização.

6.4.3 GERENCIAMENTO DE VULNERABILIDADES

Por meio de uma interface moderna com visualizações no painel de relatórios, vamos apresentar a evolução das execuções e avaliações dos resultados seguindo as estruturas das práticas recomendadas.

6.4.4 VISIBILIDADE DO MUNDO CLOUD.

Com a visibilidade e avaliações contínuas em ambientes de nuvem pública. Os Cloud Connectors identificam automaticamente os ativos no Amazon Web Services, no Microsoft Azure e no Google Cloud Platform e monitoram seu status em tempo real.

Entre outras características e funcionalidades, nossa plataforma permite avaliar se a sua infraestrutura está de acordo com os requisitos PCI, que permite que comerciantes e prestadores de serviços demonstrem que seus sistemas voltados a internet são seguros, de acordo com os requisitos de verificação de vulnerabilidades de rede externa do Padrão de segurança de dados (PCI DSS).

Vamos oferecer inteligência, alertas e conselhos de segurança de alto nível. Nosso foco em garantir que as verificações de vulnerabilidades, pesquisas de dia zero e benchmarks de configuração mais recentes sejam disponibilizados imediatamente para ajudar a proteger sua infraestrutura e sistemas.

6.5 SOC

O Security Operations Center (SOC) da Think IT é um serviço de segurança para a TI para empresas no modo 7/24/365, trabalhando para identificar incidente ou evento que possa afetar a segurança da organização, impactando a continuidade operacional de seus negócios e a integridade dos dados.

O SOC trabalha integrado com um conjunto de ferramentas, processos e equipe, no qual todas as ações de segurança são centralizadas e dentro de um fluxo contínuo e correlacionado, de forma uniforme para o atingimento da segurança esperada, responsável por garantir que possíveis incidentes sejam corretamente identificados, analisados, defendidos, investigados e relatados.

O nosso serviço de SOC utilizará uma solução de SIEM que foca em monitorar e analisar as atividades nos logs de servidores, bancos de dados, aplicativos, sites e outros sistemas,

procurando atividades anômalas que possam indicar um incidente ou comprometimento da segurança.

A equipe do SOC trabalha em estreita colaboração com equipes de resposta a incidentes do cliente, neste caso como apoio na mitigação os problemas de segurança sejam analisados rapidamente após a descoberta.

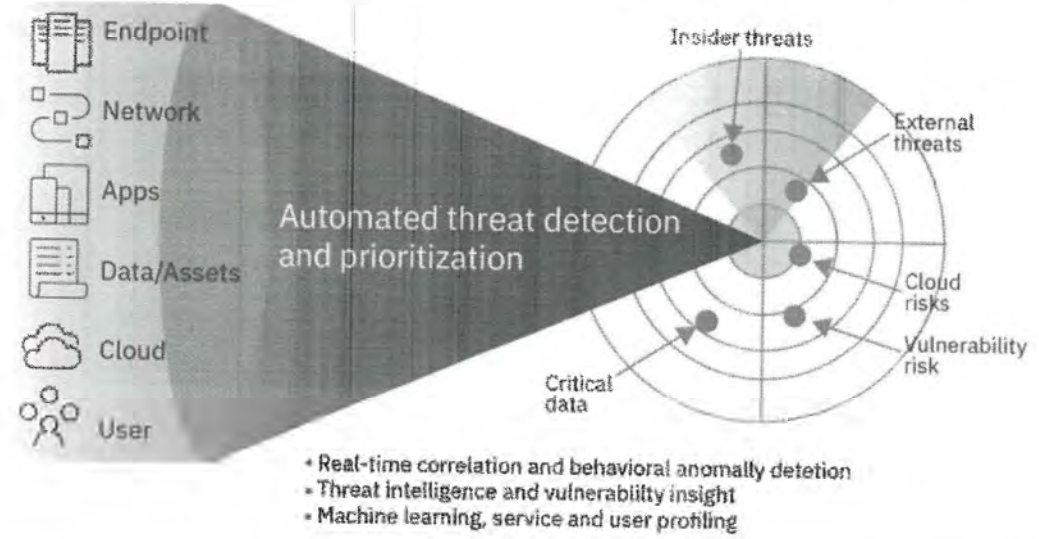
6.5.1 SIEM - INTEGRAÇÃO

Os eventos de segurança podem ser integrados a partir de: firewalls, redes virtuais privadas, sistemas de detecção de intrusão, sistemas de prevenção de intrusão, bancos de dados e muito mais

- Logs de rede: de switches, roteadores, servidores, hosts e mais
- Atividade na nuvem: De SaaS e ambientes de infraestrutura como serviço (IaaS), como Office365, SalesForce.com, Amazon Web Services (AWS), Azure e Google Cloud
- Contexto de usuário e ativo: dados contextuais de produtos de gerenciamento de identidade e acesso e vulnerabilidade scanners
- Eventos de endpoint: Do log de eventos do Windows, Sysmon, soluções EDR e mais.

6.5.2 NOSSO SIEM - DIFERENCIAL

O Security Information and Event Management (SIEM), permite que nossas equipes de segurança consigam detectar e priorizar com precisão as ameaças em toda a empresa e fornece insights inteligentes, que permitem que as equipes respondam rapidamente para reduzir o impacto de incidentes. Ao consolidar eventos de log e dados de fluxo de rede de milhares de dispositivos, terminais e aplicativos distribuídos por toda a rede, o SIEM correlaciona todas essas informações diferentes e agrega eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes



6.5.3 CARACTERISTICAS - ARQUITETURA

- Atendemos 100% dos itens de arquitetura mencionados no Termo de Referência, acrescentando algumas funções importantes:
- Nossa solução é 100% integrada, permitindo a melhor correlação de logs e análises de comportamentos com uso de Inteligência Artificial e pesquisa de dados em várias fontes de Segurança da Informação ao redor do mundo dos principais provedores.
- Toda a solução de SIEM será sobre a responsabilidade da Think IT, no qual será suportada, gerenciada e responsável por todas as manutenções, bem como manter o relacionamento direto com o fabricante.
- A nossa arquitetura prevê a instalação de um virtual Appliance dentro do datacenter da **SPTrans** que trabalhará como Gateway, executará a centralização dos logs integrados, compactando e criptografando e fará o envio dos metadados ao SOC da Think IT, reduzindo o uso de link e garantindo a análise dos dados.
- Em caso de falha de comunicação entre o datacenter da **SPTrans** e a nossa central de operações, o gateway na **SPTrans** tem a capacidade de captura e

armazenamento para após o restabelecimento realizar o envio e consolidação dos dados no SOC.

- Os limites de processamento de EPS e capacidade estão dentro do volume exigidos para suportar o aumento de até 10% no limite por até 2 horas.
- A arquitetura terá redundância na implantação dos componentes, evitando assim os riscos de parada por falha de algum componente único.
- A solução atende os requisitos de permitir desenvolvimento em caso de necessidade especial de novos plugins para integrações.
- Confirmamos o atendimento de todos os itens 5.2 e 5.3 do Termo de Referência.

6.5.4 TRATAMENTO DE EVENTOS

- Adicional aos pontos solicitados no Termo de Referência 5.4, 5.5, 5.6, no qual atendemos a todos ainda acrescentamos regulamentações externas como a SOX, atendemos todas as coletas de eventos solicitadas e incluso a lista adicional: Windows, Linux, IBM/AIX, IBM/RACF, HPUX, Solaris, Oracle Database, IBM/DB2, MS SQL Server, Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet e Palo Alto e SonicWall), Network IPS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee);
- Nossa ferramenta integra de forma automática os resultados do scan de vulnerabilidade, incorporando na correlação de dados adicionando informações importantes de fontes diferentes.
- Os itens 5.7 de Armazenamento de dados, será suportado com modelo redundante de discos e backup de dados, atendendo todos os itens.

6.5.5 GERENCIAMENTO E OPERAÇÃO

- Atendemos a totalidade no atendimento aos itens 5.8 e 5.9 e acrescentamos que nossas instalações estão sobre um duplo controle de acesso aos profissionais, nossos profissionais são treinados e organizados sobre as diferentes torres de conhecimento e responsabilidades descritos no serviço item 7 a seguir.

6.5.6 COMPATIBILIDADE E ESCALABILIDADE

- Atendemos a totalidade das solicitações do item 5.10 e disponibilizamos mais algumas tecnologias homologadas da plataforma e solução de SIEM, essas tecnologias estão homologadas e disponíveis, são inclusas e inseparáveis que podem ser úteis em caso de alteração, aquisição de novas arquitetura de TI pela **SPTrans**, sem nenhum custo ou ônus adicional.

COMPATIBILIDADE.

- Microsoft Windows;
- IBM AIX;
- IBM zOS;
- IBM AS400;
- HP-UX;
- Sun Solaris;
- Servidor Web e Proxy
- Microsoft IIS;
- Apache;
- NGinX Proxy Reverso;
- Squid Web Proxy;
- BlueCoat SG;
- IronPort Security Web Security;
- Websense
- McAfee Web Gateway;
- Roteadores/switches
- 3com;
- Nortel;
- Extreme;
- Enterasys;
- Cisco;
- Juniper;
- Aruba;
- Servidor de Banco de dados e Ferramentas de DAM
- Oracle;

- Microsoft SQL;
- DB2;
- IBM Guardium
- Imperva SecureSphere
- Scanners de vulnerabilidades
- Nessus;
- QualysQuard;
- Foundstone;
- NMAP;
- Concentrador VPN;
- NORTEL;
- Check point UTM;
- Cisco;
- Serviços em Nuvem
- Amazon AWS CloudTrail
- Amazon VPC Flow
- Amazon GuardDuty
- Microsoft Azure
- Microsoft Office 365
- Akamai
- Cisco Umbrella

6.5.7 MATRIZ DE RESPONSABILIDADE SOC

A Matriz de Responsabilidade a seguir indica a responsabilidade por determinados processos, atividades e tarefas listadas como parte dos serviços do escopo desta proposta, a ideia não e a exaurir todas as possibilidades, mas garantir o entendimento das principais responsabilidades, essas poderão ser ajustadas, ampliadas em tempo de contrato.

As informações em ambas as colunas indicam uma responsabilidade combinada ou esforço combinado entre as partes. (R) responsável, (A) apoio (C) Consultado e (I) informado

Monitoramento - SOC	THINK IT	SPTrans
Manter e aprimorar a ferramenta de console central do SIEM	R	
Realizar a monitoração com uso do SIEM e SCAN de vulnerabilidade e seus componentes contidos no baseline, visando ações proativas, incluindo identificação de vulnerabilidades.	R	I
Escalonar a equipe solucionadora do fornecedor ou da **SPTrans** em caso de incidentes.	R	I
Gerir, manter e controlar a comunicação, com informações relevantes aos serviços, específicos ao Ambiente de TI, atualizados em períodos determinados no escopo de relatórios pré-determinado neste contrato.	R	I
Recomendar novas métricas usadas para monitoramento de segurança.	R	IC
Ajustar mudanças nas rotinas de monitoramento.	R	I
Aprovar quaisquer exceções e alterações aos padrões.	R	IC
Monitoração dos principais itens para garantia dos serviços de equipamentos e sistemas deste Termo de Referência.	R	
Propor melhorias e implementá-las quando aprovadas pela gestão **SPTrans** nas ferramentas do escopo desta proposta e integração dos serviços;	R	
Realizar o ***escalation e notification*** (E&N) dos itens críticos e impactantes à operação conforme processo acordado.	R	I
Realizar a Operação, Execução, Monitoração (Proativa) e Gerenciamento do SIEM , bem como seus respectivos softwares de controle do SOC.	R	
Registro sistemático das ocorrências de falhas no serviço do contrato.	R	I
Resolução dos incidentes no ambiente de produção da **SPTrans** nos diversos ambientes através da intervenção direta ou acionamento do fornecedor responsável.	C	R
Responsável em aprovar as ações emergenciais que possam ter impacto na disponibilidade do ambiente de produção da **SPTrans**.	A	R

Apresentar relatório de problemas, RCA, e a proposta de solução ou contorno para incidentes críticos de Segurança da Informação no escopo desta proposta.	R	A
Resolução de problemas nos sistemas corporativos da **SPTrans.**		R
Monitorar e avaliar o que atualizar nos sistemas operacionais e outros softwares avaliados, direcionando proposições de solução e ou mitigação.	R	

Gerenciamento de Mudança	THINK IT	SPTrans
Realizar a Supervisão, o acompanhamento e a execução (quando necessário) de procedimentos operacionais de manutenção, incluindo atualizações de patch e de versões de programas.		R
Realizar a abertura de solicitação de mudanças relativas ao ambiente da **SPTrans** para manutenção, ajustes dos ativos, softwares e equipamentos deste contrato.	A	R
Realizar abertura e acompanhamento das mudanças para novas atualizações dos softwares onde a origem é caracterizada pela necessidade evolutiva ou de atualização de aplicativos sobre responsabilidade da equipe da THINK no escopo desta proposta.	R	I
Aprovação das janelas de manutenção normais e emergenciais.	R	A
Acompanhamento da evolução da janela e comunicação do status versus o planejamento.	R	
Tomada de decisão sobre continuidade da janela e análise de impacto ao negócio.	A	R

Segurança da Informação	THINK IT	SPTrans
Planejamento das atividades para execução do SCAN de vulnerabilidade	R	CI
Mapeamento dos ambientes e sistemas a serem realizado o scan	R	A
Execução do scan para obter Diagnóstico das fragilidades tecnológicas;	R	
Implantação da tecnologia de SIEM para monitoramento do escopo desta proposta	R	I

Gestão dos eventos de segurança da informação em regime 24 x 7 com apoio da equipe		
(*) Suportar a **SPTrans** na investigação e atuação em eventos de Segurança da informação	R	A
Reuniões de equipes técnicas para apresentação de relatórios técnicos, esclarecimento de dúvidas	R	A
Validação das correções de falhas e vulnerabilidades	R	A
Executar as ações de correção do ambiente	I	R

(*) o contrato suportará na investigação e atuação de eventos de Segurança da informação, através de log, gestão de identidade, antivírus, regras de firewall.

6.5.8 HORÁRIO E LOCAL DE ATENDIMENTO SOC

Os conceitos e parâmetros dispostos na tabela abaixo balizarão a prestação dos serviços e darão base à apuração dos níveis de serviço gestão do SOC:

TIPO	Descrição	Horário de atendimento
Requisição de serviço	Qualquer solicitação ou demanda de serviço que não seja ocasionada por uma falha na infraestrutura de TI	9x5
Evento	Alarme gerado pela ferramenta de monitoração, indicando uma interrupção ou um desvio do funcionamento normal	24x7x365
Incidente	Qualquer evento que represente uma interrupção do serviço ou uma redução da qualidade do serviço	24x7x365
Problema	Causa desconhecida de um ou mais incidentes.	Análise de causa-raiz e Plano de ações: 9X5 Execução de mudança para correção do problema: conforme o planejamento da mudança

Mudança	Atividade programada com a finalidade de resolver um problema ou com ação proativa para evitar incidentes	Planejamento da mudança: 9X5 Execução de mudança para resolução de problema: conforme o planejamento da mudança

6.6 PEN TEST E SERVIÇOS TÉCNICOS ESPECIALIZADOS

A realização das reuniões conjuntas entre os profissionais da **THINK IT** e do cliente se darão em horário comercial, em datas e horários agendados previamente, em comum acordo entre todos os participantes.

6.7 WAF

Com os ataques de camada de aplicativo em ascensão, a Think com a plataforma da Verizon ajuda a proteger seus aplicativos web e os dados dos usuários com um WAF corporativo com grande capacidade de processamento.

6.7.1 PROTEÇÃO DUPLA

O WAF disponibiliza proteção dupla. A ferramenta da Verizon é habilitada a implementar Web Application Firewalls de tempo integral. Esse recurso essencial minimiza os falsos positivos, testando as mudanças de regra em modo de auditoria contra o tráfego de produção, enquanto protege os sites e a infraestrutura usando regras testadas. O resultado é produtividade e proteção ao mesmo tempo.

6.7.2 CONFIGURAÇÕES ALTAMENTE GRANULARES E AMPLAS

Personalize defesas para perfis específicos de ameaças, interrompendo os atores maliciosos enquanto permite que os usuários legítimos acessem sites e aplicativos. Conjuntos amplos de regras abrangem inúmeras vulnerabilidades de aplicativos, dentre elas:

- Injeção de SQL (SQLi)

- Cross-Site Scripting (XSS)
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)
- Injeção de objeto PHP
- Execução de código remoto (RCE) e muitos outros

6.7.3 PROTEÇÃO CAMADA DE APLICAÇÃO.

Habilite um conjunto abrangente de medidas de detecção de ameaças com o objetivo de identificar tráfego malicioso. Essas medidas definem os tipos de ataques à camada de aplicativo que serão detectados, como:

- Validação de protocolo
- Identificação de cliente malicioso
- Assinaturas genéricas de ataque
- Assinaturas de vulnerabilidades conhecidas
- Acesso por Trojan / backdoor
- Negação de serviço

Filtrar o tráfego indesejado por meio da seleção de um perfil de entrega personalizado.

O tráfego que não atende aos requisitos definidos neste perfil de entrega HTTP pode ser bloqueado antes mesmo de atingir nossa rede principal.

Estabelecer restrições de tráfego para bloquear tráfego malicioso.

Use uma lista de permissão, lista negra ou lista de acesso para restringir o tráfego por ASN, país, endereço IP, referenciador, URL, agente de usuário, método HTTP, tipo de mídia e / ou extensão de arquivo.

7 GESTÃO DE SERVIÇOS.

7.1 SERVICE DELIVERY

É a área que faz a interface direta com os clientes. Formada por profissionais experientes, chamados "*Service Delivery Managers*", é responsável por garantir a excelência do atendimento ao cliente, através de ações contínuas que visam manter e aperfeiçoar o nível dos serviços prestados. Atua como representante do cliente dentro da **THINK IT**, traduzindo as necessidades de negócio e decisões estratégicas para os times internos.
O Recurso estará à disposição da **SPTrans,** para ações corporativa, negócios e com participação em reunião com atendimento presencial ou através de e-mail e telefone.

7.2 CENTRAL DE OPERAÇÕES - SOC

Área responsável por acompanhar, em tempo real, os ambientes gerenciados, atuando como um ponto único de contato com o cliente e a área de relacionamento. É responsável por centralizar e entregar os níveis de serviço da segurança contratados. O **SOC** gerencia todos os processos e ferramentas de segurança que são a base metodológica dos serviços prestados pela **THINK IT**:

7.2.1 GESTOR DE INCIDENTES

Função organizacional responsável pela gestão do processo de Gerenciamento de Incidente, exercendo o papel de Ponto Único de Contato para detecção, abertura, comunicação, até a restauração da operação à situação padrão de normalidade. Inclui a garantia de execução das atividades do processo conforme especificadas, observância dos SLAs acordados e acompanhamento das métricas e KPIs relacionados.

Sempre que um **incidente ou evento de risco** for detectado pelas ferramentas de monitoração, um chamado será aberto na ferramenta ITSM da Think IT, a equipe de

monitoração confirmará a ocorrência do incidente e encaminhará o chamado para a equipe solucionadora da **SPTrans** e seguirá o processo de escalonamento e de notificação devido.

O objetivo do processo de gerenciamento de incidentes é restabelecer o funcionamento do ambiente o mais rápido possível, fornecendo maior disponibilidade dos sistemas para os usuários e atendendo o SLA acordado. Para isso, pode ser necessária a implementação de uma solução de contorno em vez de uma solução definitiva.
No caso de um alerta, um ticket de incidente será aberto na ferramenta ITSM e a equipe de monitoração fará o escalonamento e notificação das equipes de Operações e Suporte de Segurança da **Think IT** e da **SPTrans** ou seus fornecedores para atendimento responsável para a correção do incidente, seguindo o documento de escalação a ser desenvolvido durante a fase de Implantação dos serviços.

A **THINK IT** será responsável pela monitoração ativa e proativa de segurança dos recursos de Tecnologia da Informação e Telecom da **SPTrans** hospedados em data center próprio e em nuvem pública, no regime 24x7x365.

A monitoração será feita remotamente a partir da sede da **THINK IT**, no CENESP (Centro Empresarial São Paulo), através de uma VPN ou outro meio seguro entre as redes da THINK IT e da **SPTrans.**

A nossa solução atende o de tratamento dos incidentes identificados pelas regras de correlação, conforme descrito no item 5.9 do Termo de Referência.

- Permite associar os incidentes aos usuários da solução;
- Permite encerrar um incidente quando este for solucionado;
- Permite adicionar anotações aos incidentes para registro das ações tomadas ou observações;
- Permite 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;

- Possui integração suportada na solução, com ferramenta especializada no tratamento de resposta à incidente;
- Permite 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.

7.2.2 OPERAÇÃO DO SOC

Equipe responsável pela execução e acompanhamento de procedimentos pré-determinados.

Como parte do escopo de serviços requeridos pela **SPTrans**, a **THINK IT** fará o monitoramento em regime 24x7x365. Como principais responsabilidades, temos:

- Monitoração proativa, gerenciamento de eventos, troubleshooting;
- Garantia e controle de qualidade dos serviços de operação do SOC.

Entre as atividades a serem realizadas pelas equipes de operação, destacam-se:

- Realizar a Operação, Execução, Monitoração (Proativa) do Gerenciamento do SIEM no SOC bem como seus respectivos softwares de controle;
- Gerir, manter e controlar um Quadro de Aviso, com informações relevantes aos serviços, específicos ao Ambiente de TI, atualizados em períodos semanais e/ou por demanda da **SPTrans**;
- Criar e manter os documentos com as rotinas de processos e procedimentos de apoio à Operação (Knowledge base). Estes documentos devem estar disponibilizados em locais previamente definidos, de comum acordo entre a **THINK IT** e a **SPTrans**;
- Comunicar as eventuais falhas de segurança que venham comprometer a **SPTrans**;

7.2.3 GESTÃO DE PROBLEMAS

Função organizacional responsável pela gestão do processo de Gerenciamento de Problema, exercendo o papel de identificação, abertura e encaminhamento de Problemas

para os responsáveis pela análise e investigação de causa raiz. Inclui a garantia de execução das atividades do processo conforme especificadas, progressão do ciclo de vida dos Problemas e acompanhamento das métricas e KPIs relacionados.

Enquanto o gerenciamento de incidentes tem por objetivo restabelecer o funcionamento do ambiente o mais rápido possível, o objetivo do processo de gerenciamento de problemas é evitar que os incidentes ocorram. Dessa forma, o gerenciamento de problemas atua nos seguintes casos:

- Análise de causa raiz e definição de uma solução definitiva para um incidente resolvido através de uma solução de contorno;
- Análise de causa raiz e definição de uma solução para um incidente que se repete múltiplas vezes (reincidência);
- Análise de causa raiz e definição de uma solução para um incidente crítico.

7.2.4 GESTÃO DE REQUISIÇÕES

Função organizacional responsável pela gestão do processo de Gerenciamento de Requisição de Serviço para as solicitações rotineiras e de serviços padronizados. Responde pelas atividades de abertura de solicitações provenientes de várias fontes. Executa comunicação, encaminhamento e monitoramento do ciclo de vida das Requisições de Serviço. Inclui a garantia de execução do fluxo do processo conforme especificado, observância dos prazos acordados e acompanhamento das métricas e KPIs relacionados.

7.2.5 GERENCIAMENTO DE MUDANÇAS

O objetivo do gerenciamento de mudanças é permitir que as mudanças sejam efetuadas no ambiente causando o menor impacto possível para os usuários. As mudanças podem ser provocadas por uma solicitação, por uma necessidade de atualização técnica, para correção de um problema ou para implementação de uma melhoria ou de um novo sistema, e podem ser classificadas como normais, padrão ou emergenciais.

As mudanças consideradas como padrão são mudanças pré-aprovadas, pois não causam nenhum impacto e tem um risco muito baixo, como uma mudança de senha ou a instalação

de uma nova estação de trabalho. Estas não necessitam ser registradas como mudança e não precisam passar pelo comitê consultivo de mudança (CAB, na sua abreviação em inglês).

As mudanças normais são aquelas que precisam ser planejadas com antecedência para validação técnica, janela de execução e precisam passar pelo CAB.

As mudanças emergenciais são aquelas que não são agendadas, precisam ser implementadas imediatamente para resolução de incidentes críticos, mas que têm um impacto e um risco significantes. Por essa razão, devem ser documentadas e passar por aprovação do comitê consultivo de mudança emergencial. Em geral, este comitê é um subgrupo do comitê consultivo de mudança.

7.2.6 GERAÇÃO DE RELATÓRIOS E KPI

Função organizacional responsável pelo desenvolvimento e provisão de informações gerenciais, gráficos e relatórios de indicadores e métricas (diários, semanais e mensais). Essas informações são utilizadas em todos os processos de gerenciamento de serviços visando o atingimento dos objetivos dos contratos e requisitos de serviço previamente definidos.

A equipe de Gestão da Qualidade será responsável por analisar as métricas e resultados dos relatórios mensais, publicar os resultados e prover feedback para a equipe, buscar e implementar soluções de melhorias, verificar a eficiência das melhorias implementadas, garantir a qualidade do atendimento e do registro das informações nos chamados, fazer auditorias internas para garantir a entrega.

7.2.7 SUPORTE ESPECIALIZADO

Função organizacional especializada nas várias tecnologias designadas para execução de requisições de risco ou maior complexidade, responsável pelo papel de suporte em nível especialista sênior para restauração de Incidentes complexos e para investigação de Problemas que demandem conhecimento tecnológico especializado.

7.3 GERÊNCIA DE PROJETOS

Equipe formada por gerentes que respondem pela condução dos projetos executados pela **THINK IT**, responsável pelo planejamento das atividades, alocação e coordenação das equipes, interlocução com os clientes, status report sobre o andamento dos projetos, gestão de escopo, aplicação da metodologia e garantia da qualidade dos produtos gerados.

7.4 ESPECIALISTAS NA IMPLANTAÇÃO DE PROJETOS

Função organizacional responsável pela implementação técnica dos projetos, formada por especialistas certificados nas diversas tecnologias demandadas.

7.5 PROCESSOS E QUALIDADE

Área responsável pela especificação, implementação, auditoria e ações de aperfeiçoamento dos processos de Gerenciamento de Serviços dentro da **THINK IT**. Responde pela definição das métricas e indicadores necessários para aferição da execução, garantia dos objetivos dos processos e atingimento dos níveis de serviço acordados. Possui isonomia na aferição dos controles e relatórios para identificação de planos de ação de melhoria contínua para as demais áreas e funções.

7.6 IMPLANTAÇÃO

Com foco em **minimizar impactos** e **otimizar a entrega** dos serviços, a **THINK IT** desenvolveu um **Modelo de projeto seguro** e **consistente**, contemplando as atividades essenciais para uma adequada transferência dos serviços.

A experiência adquirida por meio da execução de centenas de projetos de serviços e migrações de ambientes críticos e complexos mostra que estas atividades devem ser minuciosamente planejadas e detalhadas. Toda etapa de Implantação deve ser tratada como um projeto, contemplando planejamento, equipe dedicada para execução e gestão, processo de acompanhamento e comunicação e um plano minucioso de mitigação e contingência. Assim, as tarefas de Implantação estão baseadas num modelo que agrega

não só nossa vasta experiência em projetos dessa natureza, mas também as melhores práticas de gerenciamento de projetos, que tem por objetivo final, garantir: **mínimo impacto**, **comunicação contínua**, **parceria** e **flexibilidade** na abordagem.

7.6.1 FRAMEWORK DE PROJETO

Esse **Framework** é composto de:

- Uma **metodologia** de gestão de projetos, e;
- Um **frame** de aspectos relevantes a ser trabalhado durante todo projeto

Para melhor ilustrar, na figura abaixo destacamos as etapas e as principais atividades a serem realizadas em cada uma delas, segundo a nossa **metodologia** de gestão de projetos, que visa entregar os seguintes **aspectos**:

- Comunicação
- Gestão e Governança
- Operações

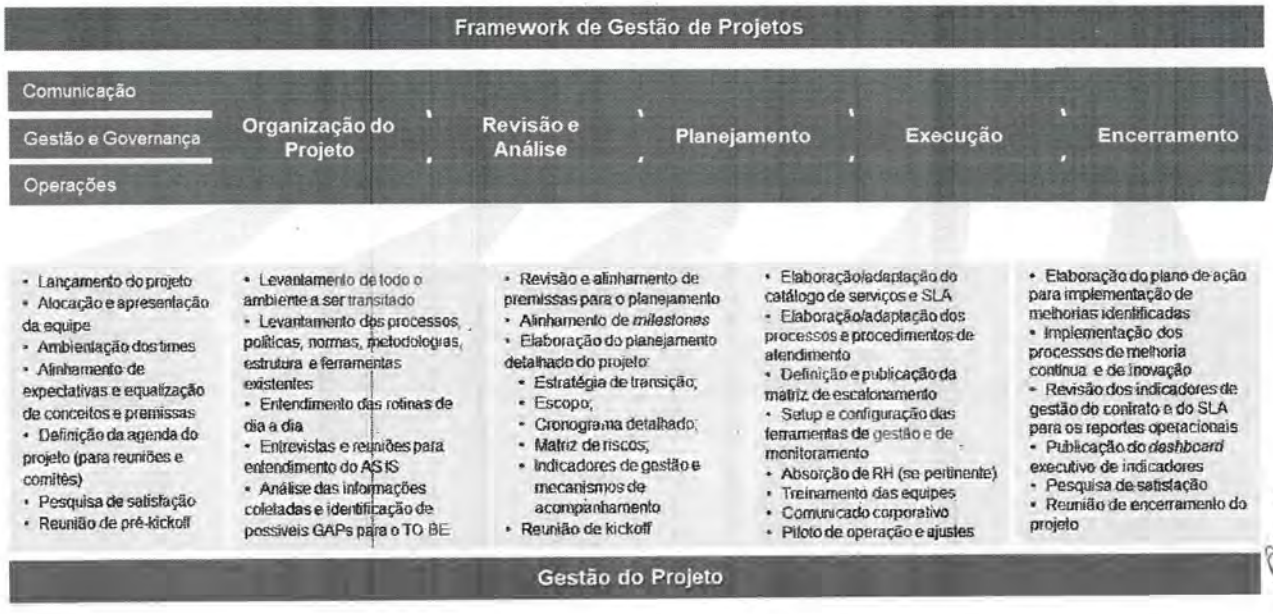


Figura 8 – Framework de Gestão de Projetos

Os aspectos **do frame** a serem trabalhados e entregues ao longo de todas as etapas da nossa metodologia de projeto são os seguintes:

1. **Comunicação:** Determina e implementa o plano de comunicação **durante todo o projeto**, gerenciando as informações a serem divulgadas a todos os envolvidos. Etapa de extrema importância que deverá ser executada a 4 mãos, em conjunto com a equipe da **SPTrans.** A boa execução do plano de comunicação garantirá o alinhamento e o engajamento de todos os envolvidos no projeto.

Principais atividades:

- Identificar pessoas chave da **SPTrans** e outros fornecedores existentes que participam dos processos pertinentes ao projeto;
- Estruturar um repositório para armazenamento de relatórios, procedimentos, matrizes de escalonamento e de acionamento, formulários e checklists;
- Fornecer o nível certo de comunicação para o público correto para suavizar temores ou inseguranças e para minimizar a interrupção do negócio;
- Certificar que os processos apropriados e as linhas de comunicação existam entre a unidade de operação de serviços e os envolvidos no projeto;
- Acordar reuniões, mecanismos de comunicação e programação de entrega de relatórios;
- Criar um ambiente contínuo para comunicações abertas e honestas com participação tanto da **THINK IT** quanto de pessoas chave da **SPTrans.**

2. **Gestão e Governança:** Tem por objetivos identificar o nível de serviço atual, definir e implementar os novos processos de gestão dos serviços bem como o SLA (*Service Level Agreement*), o SLO (*Service Level Operational*) e a estrutura de reporte para a monitoração dos indicadores de serviços. Este aspecto cuida de definir e implementar todos os processos e mecanismos de gerenciamento e de governança do contrato.

3. **Operações:** Etapa responsável por levantar as necessidades da operação existente, estruturar os processos e implementar o serviço, além de buscar a estabilização e

segurança deste. O objetivo deste aspecto é garantir que todas as atividades pertinentes ao estabelecimento da operação sejam executadas.

- Principais Atividades:
  - Desenvolver e acordar os processos e os procedimentos para as operações de segurança;
  - Identificar e acordar as ferramentas necessárias para implementar o modelo de processo;
  - Efetuar se necessário workshop para firmar o fluxo integrado de processos definidos e implementados;
  - Definir o processo de aceitação (critérios de aceitação operacional) e garantir a aprovação formal da **SPTrans**;
  - Definir papéis e responsabilidades claros para cada parte interessada;
  - Desenvolver a estratégia da operação contínua, e planejar a entrega dos objetivos acordados;
  - Desenvolver e implementar a estrutura para mensurar e reportar indicadores da operação de serviços;
  - Estabelecer uma estrutura de qualidade baseada nos padrões selecionados para os processos definidos;
  - Desenvolver e implementar um modelo para a melhoria contínua da unidade.
  - Fornecer a todas as pessoas a quantidade adequada de treinamento e transferência de conhecimento no tempo certo;
  - Gerenciar a transferência da carga de trabalho para minimizar o impacto sobre a continuidade dos serviços;
  - Manter os principais processos do negócio, o conhecimento do cliente, o conhecimento de políticas e o conhecimento das aplicações;
  - Manter níveis de serviço, assegurar interrupção mínima durante o período de Estruturação/Implantação;
  - Certificar que as pessoas estejam preparadas em menos tempo e que estejam desempenhando as novas funções com sucesso;
  - Documentar os principais processos de negócio e o conhecimento das aplicações;

- Acordos de Nível de Serviço (SLA) e Manual de Operações: assegurar que os níveis de serviços e métricas de serviço estão documentados, incluindo os Acordos de Nível de Serviço (SLA) e o Manual de Operações em conjunto com o processo e fluxos de procedimento;
- Estabelecer relatórios de nível de serviço;
- Mecanismos de comunicação: Acordar reuniões, mecanismos de comunicação e programação de relatórios de entrega;
- Preparar o **SOC THINK IT** para a operação da **SPTrans**;
- Integrar os processos de ITSM de acordo com as necessidades **SPTrans**

7.6.2 ORGANIZAÇÃO DO PROJETO

A **THINK IT** disponibilizará uma equipe dedicada para execução das tarefas de Implantação, além dos especialistas necessários que trabalharão em parceria com as equipes alocadas. A estrutura da equipe de Implantação é apresentada a seguir:

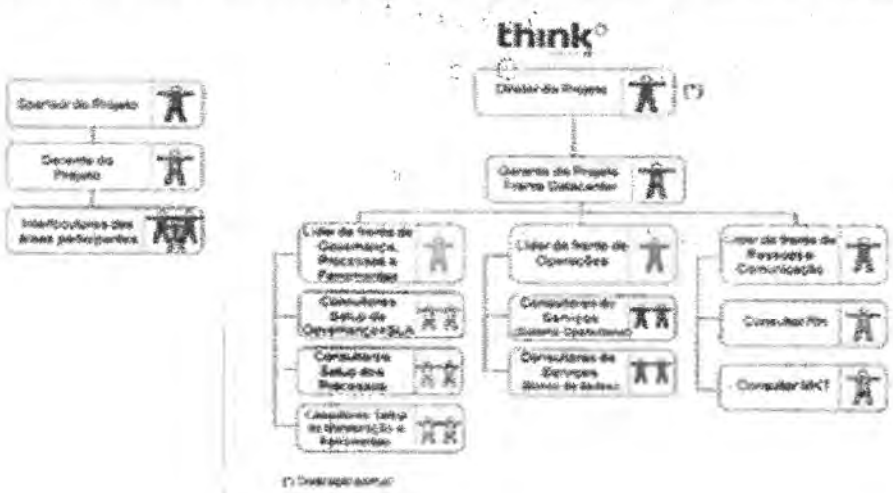


Figura 9 – Organograma da base Implantação

(*) O percentual de dedicação de cada participante da equipe será definido na etapa de detalhamento do Plano do Projeto.

No diagrama acima, os papéis de Implantação **THINK IT** são temporários e serão desalocados conforme os serviços estiverem em operação plena.
Em linha com o **Framework** apresentado acima, a equipe de Implantação do Projeto atuará com foco em estabelecer a Governança e a Gestão dos Serviços, as Operações (com os respectivos Processos, Ferramentas e Pessoas) e a Gestão da Comunicação para garantir o alinhamento, o envolvimento e o engajamento de todos.

8 GOVERNANÇA E PROCESSOS

8.1 CONCEITOS

A fim de garantir um correto entendimento e alinhamento dos **conceitos** que fundamentam a definição do SLA, dispomos na tabela abaixo, os parâmetros com seus respectivos descritivos e fontes de coleta, que balizarão a prestação dos serviços e darão base à apuração dos níveis de serviço:

Parâmetro	Descritivo	Fontes de coleta
Disponibilidade	A disponibilidade de um serviço é o percentual de tempo correspondente ao serviço disponível para os usuários, dentro do horário planejado.	Será medido utilizando as informações contidas na ferramenta de monitoração do ambiente (TMS).
Tempo médio de atendimento para incidentes ou problemas	É o tempo de atendimento dado a uma incidência ou falha. É medido desde o momento em que o problema é informado pela **SPTrans**, ou **percebido pela equipe de monitoração/operação**, até o momento em que ocorre o primeiro contato.	Será medido utilizando os registros existentes na ferramenta de gestão de chamados .

Adicionalmente e para balizamento de entendimento, em conformidade com os conceitos preconizados pelo **ITIL**, destacamos as seguintes definições a serem consideradas na composição do SLA:

Conceito	Definição
Incidente	Qualquer evento que não é parte padrão da operação de um serviço, que causa ou pode causar uma interrupção ou redução da qualidade do serviço
Problema	Causa desconhecida de um ou mais incidentes
Service Request (ou Solicitações)	Qualquer solicitação/demanda que não seja a analise e monitoramento de uma falha na segurança da informação.
Eventos	Eventos de monitoração

8.2 SEVERIDADE SOC

Severidade é o grau do impacto causado por uma parada ou interrupção nos serviços da **SPTrans**, cuja operação, gestão e administração são objetos desta proposta.

O conceito de **Severidade** servirá para estabelecimento dos parâmetros de "Tempo médio de atendimento de incidentes ou problemas", "Tempo médio de notificação de problemas" e "Tempo médio entre Problemas", uma vez que, eles serão definidos em função do grau de severidade identificado e do SLA acordado com a **SPTrans**.

O grau de Severidade de um chamado será atribuído de acordo com a extensão das consequências dos impactos.

A classificação a seguir, mostra as principais condições de severidade causadas pela ocorrência de problemas e/ou interrupções em sistemas ou serviços:

Severidade	Descrição
Severidade 1 (Crítica)	Produção indisponível. Parada de componentes que resultam na indisponibilidade do ambiente da **SPTrans**. A interrupção dos serviços pode resultar em perda de negócios, receitas, multas aplicadas a **SPTrans** e comprometer prazos.
Severidade 2 (Alta)	Produção impactada. Um componente não crítico está indisponível, com problemas de performance ou operando com falhas, provocando uma disponibilidade parcial, problemas de performance ou instabilidade no ambiente da **SPTrans**.
Severidade 3 (Média)	Parada de componentes que oferecem riscos ao ambiente da **SPTrans**, como queda de redundância ou utilização de sistemas alternativos. Ocorre uma degradação de nível de serviço aceitável, com impacto mínimo, podendo ser agendada manutenção posterior.
Severidade 4 (Baixa)	Dúvidas técnicas ou solicitações, administrativas ou ocorrências que exigem novas soluções, solicitações de mudança, monitoramento e acompanhamento de eventos.

8.3 NÍVEIS DE SERVIÇO

Entende-se por um Acordo de Nível de Serviço (SLA), o grupo de indicadores previamente estabelecidos para medir a qualidade mínima e aceitável dos serviços, com medições e alcances fixados para cada um desses indicadores.

Abaixo relacionamos o acordo de nível de serviço (ANS) que irá balizar a prestação de serviços à **SPTrans**, e as respectivas penalidades por não cumprimento do nível de serviço. Os itens descritos não alteram nenhum SLA descrito na TR.

8.3.1 ATENDIMENTO E GESTÃO

Item	Máximo Permitido	KPI
Entrega de relatórios Mensais	10 dias após término do mês	100%

8.3.2 HORÁRIO DE COBERTURA DOS SERVIÇOS

Item	Cobertura
Incidentes	24x7x365
Execução de mudanças	9x5
Planejamento de mudanças	9x5
Problemas (RCA)	9x5
Atendimento de requisição de serviços	9x5
Detecção de incidentes (monitoramento)	100%

9 BASELINE

Com base nos dados fornecidos no anexo I, os seguintes volumes foram extraídos para a o entendimento da necessidade do ambiente **SPTrans**.
Os volumes serão confirmados em levantamento durante o projeto de implantação.

9.1 VOLUMES

Descrição	Quantidade
AD/Auth, DHCP, DNS	10
Servidor de Web e Mail	2
Windows e Linux de uso geral	150

Antivírus, Anti-Malware	2
Servidores de banco de dados	20
Servidor Proxy e pequenos Firewalls de borda	8
Switch Core e Firewalls de alto volume	4
IDS, IPS, VPN, LB	4
Roteadores e Switches	60
URLS:\\Aplication	20

Volumes para o atendimento:

Descrição	Quantidade
Testes de Intrusão	Recorrente.
Retestes de validações	Recorrente
SOC – Eventos por Segundo	1500

10 PREMISSAS

10.1 GERAL

São requisitos a serem atendidos pelos profissionais das equipes técnica e administrativa da THINK IT:

1. Implementar boas práticas de Segurança da Informação para garantia do mais completo e absoluto sigilo sobre quaisquer dados, materiais, pormenores, documentos, especificações técnicas e comerciais e inovações que venham a ter conhecimento ou acesso ou que venham lhe ser confiados em razão dos serviços contratados.
2. Prestar os serviços contratados com zelo e eficiência.

3. Designar e executar os serviços contratados somente por profissionais devidamente qualificados e plenamente habilitados para a função desempenhada, bem como atender instruções, normas de condutas, procedimentos e ou orientações expedidas pelo cliente por escrito, bem como aquelas que por circunstâncias específicas tiverem sido verbalmente manifestadas.
4. Cuidar da disciplina de seus colaboradores, bem como observar as normas administrativas e de segurança, substituindo qualquer de seus empregados que mantiver conduta irregular ou inconveniente.
5. Atender aos regulamentos internos do estabelecimento do cliente quanto à entrada e saída de veículos, empregados, prepostos e/ ou contratados da Think IT, sendo que o trânsito e a permanência apenas se darão nos locais e pelo tempo expressamente autorizados.
6. Repudiar quaisquer ações de seus colaboradores e prepostos que direta ou indiretamente se caracterizem como preconceituosas com relação à origem, raça, religião, classe social, sexo, cor, idade, profissão, formação, necessidades especiais ou, ainda, quaisquer outras formas de discriminação contra profissionais do cliente ou seus prepostos.

São requisitos a serem atendidos pelos profissionais do cliente durante a execução das atividades contratadas:

1. Fornecer em tempo hábil acesso às informações necessárias para a execução das atividades contratadas.
2. Agendar e assegurar a realização de reuniões de profissionais da THINK IT com pessoas chaves (*stakeholders*) para execução das atividades contratadas, com tempo de duração suficiente e em tempo hábil de maneira a permitir o cumprimento dos prazos conjuntamente definidos.
3. Analisar os documentos parciais e finais entregues pela THINK IT, decorrentes das atividades contratadas, apresentando correções que se fizerem necessárias, em tempo hábil e objetivamente organizadas, de maneira a permitir o cumprimento dos prazos conjuntamente definidos.

4. Repudiar quaisquer ações de seus colaboradores e prepostos que direta ou indiretamente se caracterizem como preconceituosas com relação à origem, raça, religião, classe social, sexo, cor, idade, profissão, formação, necessidades especiais ou, ainda, quaisquer outras formas de discriminação contra profissionais da THINK IT ou seus prepostos.

- Assumimos que a equipe da **SPTrans** ou seus fornecedores estarão disponíveis para o Projeto de Implantação nas datas acordadas na fase de planejamento. Assumimos que atrasos na entrega da solução devido a indisponibilidade dos recursos da **SPTrans** ou seus fornecedores a THINK IT não poderá ser penalizada.

10.2 PREMISSAS TÉCNICAS

- Para fornecer os serviços será necessário ter acesso aos servidores com endereço IP privado, será necessário configurar uma VPN entre a rede da **THINK IT** e cada um dos segmentos virtuais de rede da **SPTrans** nas nuvens públicas contratadas por ela.
- Será necessária a criação de uma máquina virtual no ambiente da SPTrans-SP, para ser o concentrador de log e gateway de metadados que serão consumidos pelo SOC.
- Durante a fase de Implantação, a **SPTrans** deverá fornecer a documentação para a equipe da **THINK IT** a respeito dos ambientes e das aplicações que integram o escopo dos serviços.
- Assumimos que a **SPTrans** deverá disponibilizar equipe para acompanhamento das integrações com o SIEM.
- Nenhuma instalação de agentes ou outras alterações no ambiente da **SPTrans** será executado pela equipe da **Think IT**, somente pela equipe da **SPTrans** e ou seus fornecedores responsáveis.
- Assumimos que sempre que a **SPTrans** precisar abrir uma solicitação de serviços dentro do escopo desta proposta para a **THINK IT**, o fará por telefone com o Service Desk do SOC, ou diretamente na ferramenta ITSM do TMS (THINK Management System).

11 DIFERENCIAIS DESTA PROPOSTA

São benefícios obtidos pelo cliente com a prestação dos serviços descritos nesta proposta:

- Proteção da marca
- Identificação e possibilidade de eliminação de falhas e vulnerabilidades tecnológicas;
- Redução dos riscos e danos a reputação, geralmente imensuráveis, e aumento do controle e da segurança de sistemas de T.I.;
- Evitar multas e sanções administrativas dos órgãos reguladores.
- Identificação de vetores de risco e avaliação de prejuízos potenciais;
- Fortalecimento de uma cultura de Segurança Cibernética na organização.
- Adequação aos padrões técnicos da Lei Geral de Proteção de Dados (LGPD).

12 PRAZO PARA INÍCIO DO PROJETO

Imediato após a assinatura do contrato relativo a este escopo. Priorizando a implementação de todas as ações emergenciais de mitigação de riscos de segurança que puderem ser executadas, além do início do planejamento para as demais atividades que necessitarem de um cronograma de execução mais detalhado.

13 PRAZO PARA FINALIZAÇÃO DO PROJETO

O projeto será finalizado após 6 (seis) meses da data de lançamento.

14 PRAZO DE VALIDADE DA PROPOSTA

Essa proposta é válida por 30 (trinta) dias corridos a partir da data de elaboração.

15 INVESTIMENTO

O valor de investimento pago a título de honorários pelo cliente à THINK IT para a realização dos serviços aqui descritos no período de 6 meses será de **R$2.522.587,20** (dois milhões, quinhentos e vinte e dois mil, quinhentos e oitenta e sete reais e vinte centavos), já inclusos os impostos.

No caso de alteração de escopo, os valores dessa proposta serão alterados, não necessariamente de forma proporcional.

Abaixo apresentamos a tabela contendo a descrição, quantidade e valor unitário de cada item que compõe o valor do investimento:

think
MANAGED SERVICE PROVIDER

OBJETO:	FORNECIMENTO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, VARREDURA DE VULNERABILIDADES, TESTES DE INTRUSÃO/PENETRAÇÃO E GERAÇÃO DE RELATÓRIOS, PELO PERÍODO DE ATÉ 180 (CENTO E OITENTA) DIAS.

ITEM	DISCRIMINAÇÃO	UN	QUANTIDADE	VALOR EM R$		
				UNITARIO	MENSAL	TOTAL - 6 MESES
1	SOC MONITORAMENTO 24 X 7 SOC/SIEM	EPS	TODOS ANEXO I	-	149.772,00	898.632,00
2	SOC SCAN VULNERABILIDADE	VOLUME DE ATIVOS	280,00	62,44	17.483,20	104.899,20
3	PROTEÇÃO AVANÇADA ZERODAY SYSCAL LINUX	VOLUME DE HOST LINUX	150,00	644,46	96.669,00	580.014,00
4	TESTE DE PENETRAÇÃO	QUANTIDADE	1,00	113.715,00	113.715,00	682.290,00
5	MONITORAMENTO MARCA SPTRANS	VOLUME DE MARCA	1,00	16.047,00	16.047,00	96.282,00
6	WAF	VOLUME DE APLICAÇÕES	20,00	1.337,25	26.745,00	160.470,00
				TOTAL GERAL		2.522.587,20

EMPRESA PROPONENTE		DADOS DO RESPONSÁVEL (PROPONENTE)
RAZÃO SOCIAL:	Brasforge Comércio e Serviços em Informática LTDA	NOME: Alexandre Noel de Azevedo
CNPJ:	08.053.426/0001-15	CARGO: Vice-Presidente Comercial
ENDEREÇO	Av. Maria Coelho Aguiar, 215 – Bl. C – 3º. Andar – 05804-900	(11)99449-4783
TELEFONE:	(11) 3741-5423	

16 FORMA DE PAGAMENTO

O pagamento em favor da THINK IT pelos serviços prestados, será realizado em 6 (seis) parcelas de igual valor de R$420.431,20 (quatrocentos e vinte mil e quatrocentos e trinta e um reais e vinte centavos), com a primeira parcela sendo paga em até 30 dias. Os pagamentos das respectivas parcelas serão feitos mediante depósito em conta bancária da THINK IT, definida no momento da contratação.

17 INCLUSOS

Qualquer item constante no Termo de Referência confeccionado pela SPTrans, o qual serviu como o guia de requisitos técnicos para a elaboração desta proposta, que porventura por equívoco ou esquecimento, não esteja contemplado explicita ou implicitamente neste documento comercial, será considerado como abrangido tanto no escopo técnico como no escopo financeiro desta proposta.

18 EXCLUSOS

Nos valores apresentados nessa proposta não estão inclusos quaisquer gastos adicionais relacionados com a aquisição de equipamentos, *software*, serviços ou contratação de profissionais, necessários para a implementação parcial ou total das recomendações de Segurança da Informação resultantes dos serviços prestados.

19 AUTORIZAÇÃO

O cliente autoriza os testes de Segurança da Informação externos nos alvos indicados no escopo desta proposta, bem como a exploração em profundidade das falhas e vulnerabilidades encontradas, durante a vigência do projeto, desde já ciente de que

quantidades controladas de informação confidencial podem acabar sendo acessadas como resultado da exploração em profundidade de vulnerabilidades detectadas pela equipe da THINK IT, que fará de tudo para minimizar o acesso à tais informações e fará a imediata e correta destruição das mesmas assim que possível.

20 CONFIDENCIALIDADE

As informações obtidas durante os serviços prestados pela THINK IT para o cliente, incluindo seus recursos, procedimentos e sistemas, são tratadas como confidenciais, pelo que a THINK IT se compromete a mantê-las no mais absoluto sigilo.

Assim, reitera que se obrigam, por si, por seus sócios, administradores, funcionários, prepostos, contratados ou subcontratados a manter, durante o prazo deste contrato e após o seu término, o mais completo e absoluto sigilo com relação a toda e qualquer informação, de qualquer natureza, referente às atividades do cliente, das quais, eventualmente, venha a ter acesso por força dos serviços contratados, não podendo, sob qualquer pretexto, utilizá-las para si, divulgar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se, em caso de descumprimento da obrigação assumida, por eventuais perdas e danos e sujeitando-se às cominações legais, pelo prazo de 2 (dois) anos após o término da contratação.

A **SPTrans** reconhece que a **THINK IT** é e continuará sendo a exclusiva proprietária de suas informações confidenciais e de todas as patentes, direitos autorais, segredos comerciais, marcas registradas, especificações, desenhos, modelos, cronogramas, exemplos, ferramentas, programas técnicos e outros direitos de propriedade intelectual, a menos que a **SPTrans** e a **THINK IT** acordem de forma diversa, por escrito. Nenhuma licença ou transferência de qualquer desses direitos é concedida à **SPTrans** ou fica implícita nos termos desta proposta.

21 ASSINATURA E DADOS CADASTRAIS DA THINK IT.

Alexandre Azevedo

Vice-Presidente Comercial Think IT

Razão Social : Brastorage Comercio de Serviços em Informática Ltda

CNPJ: 08.053.426/0001-15

Endereço: Av. Maria Coelgo Aguiar, Nr.215 BL: C- 3 andar São Paulo-SP

CEP: 05805-000

ANEXO III

MODELO DE CARTA DE AUTORIZAÇÃO DE CRÉDITO

MODELO

CARTA DE AUTORIZAÇÃO DE CRÉDITO EM CONTA CORRENTE
(papel timbrado)

Local/Data

SÃO PAULO TRANSPORTE S/A
Rua Boa Vista, 236 – 2 andar
São Paulo – SP

Att.: Gerência de Finanças

OBJETO:

Assunto: CRÉDITO EM CONTA CORRENTE

Prezados Senhores

Conforme disposto no respectivo Contrato, informamos abaixo os dados bancários para que sejam efetuados os créditos relativos ao contrato.

Razão Social:

CNPJ:

Nome do Banco: Caixa Econômica Federal

Nº do Banco: 104

Nº da Agência:

Nº da Conta Corrente:

Atenciosamente

Responsável da Proponente
RG e CPF