Governo do Estado de São Paulo
Companhia Paulista de Trens Metropolitanos
Depto De Contratacoes E Compras

CARTA

CT.DFCC.157/2025

Aos
Srs. GILENO GURJÃO BARRETO - Diretor Presidente e THIAGO WALTZ ALVES - Diretor Comercial
COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP
Rua Agueda Gonçalves, 240 - Jd. Pedro Gonçalves
06760-900 Taboão da Serra SP

CONTRATO DL00925-01 / PRODESP PD024401 – Designação de Gestor

Prezados Senhores,

Comunicamos a V.Sa. que o Sr. Leonardo Marques Lopes - Chefe do Departamento de Operação de TI - DFIO, telefone (11) 3117-7103, será o responsável pela gestão do contrato em referência.

Sua função será a de coordenar os trabalhos, servindo de ligação entre V.Sas. e esta Companhia, na administração de problemas, tomando decisões técnicas e administrativas, dentro dos limites contratuais.

Atenciosamente,

REGINALDO ANTONIO DE PINHO
Chefe do Departamento de Contratações e Compras

Documento assinado eletronicamente por **Reginaldo Antonio De Pinho**, **Chefe De Departamento**, em 16/10/2025, às 15:57, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0086231823** e o código CRC **90DA4CD7**.

Contrato

CÓDIGO ÚNICO Nº 20250919526
CONTRATO DL00925-01
PROCESSO DL00925 - 386.00009348/2025-32
CONTRATO PRODESP PD024401
LEI FEDERAL Nº 13.303/2016, ART. 29, INCISO XI

CONTRATO DE PRESTAÇÃO DE SERVIÇOS CONTINUADOS, ESPECIALIZADOS EM TI – TECNOLOGIA DA INFORMAÇÃO, QUE SE CONSTITUEM DE UMA SOLUÇÃO GLOBAL AO AMBIENTE DE TI E DE SEGURANÇA CIBERNÉTICA, QUE, ENTRE SI, FAZEM A COMPANHIA PAULISTA DE TRENS METROPOLITANOS E A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP.

Pelo presente instrumento, elaborado para um único efeito, as partes abaixo assinadas, de um lado a COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM, inscrita no CNPJ sob nº 71.832.679/0001-23, Inscrição Estadual nº 113.898.614-110, com sede em São Paulo/SP, na Rua Boa Vista nº 162, 6º andar - Centro, doravante denominada simplesmente CPTM, por seus representantes legais ao final qualificados, e, de outro, a COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP, inscrita no CNPJ sob nº 62.577.929/0001-35, com sede em Taboão da Serra/SP, na Rua Agueda Gonçalves nº 240 – Jd. Pedro Gonçalves, doravante denominada simplesmente CONTRATADA, por seus representantes legais ao final qualificados, ajustam e convencionam as obrigações e compromissos recíprocos, observadas as disposições da Lei Federal n° 13.303, de 30/06/2016, do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023, do Capítulo II-B do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), da legislação pertinente, das normas internas específicas da CPTM, do Código de Conduta e Integridade da CPTM, do Código de Conduta e Integridade de Fornecedores, Prestadores de Serviços e Parceiros da CPTM, do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), com suas alterações subsequentes, bem como toda a legislação aplicável sobre privacidade e proteção de dados, inclusive, normas setoriais ou gerais sobre o tema e pela Política de Segurança da Informação da CPTM, no âmbito da execução do objeto deste Contrato, pelas condições constantes das demais normas regulamentares aplicáveis à espécie, para os fins do Processo 386.00009348/2025-32, nas condições estabelecidas nas seguintes cláusulas:

1 OBJETO

1.1 Constitui objeto do presente contrato a prestação de serviços continuados, especializados em TI – Tecnologia da Informação, que se constituem de uma solução global ao ambiente de TI e de segurança cibernética.

1.2 A presente contratação, para fins de informação à Receita Federal do Brasil, não envolve transferência de tecnologia à CPTM.

2 DOCUMENTOS INTEGRANTES

2.1 Para melhor caracterização do objeto, bem como para definir procedimentos decorrentes das obrigações ora contraídas, integram este instrumento seguintes documentos:

2.1.1 Termo de Referência (Anexo 1);
2.1.2 Proposta da CONTRATADA (Anexo 2);
2.1.3 Cronograma Físico Financeiro (Anexo 3);
2.1.4 Declaração de Ciência e Responsabilidade (Anexo 4); e
2.1.5 Termo de Confidencialidade e Uso (Anexo 5); e
2.1.6 Termo de Ciência e de Notificação (Anexo 6).

2.2 No caso de divergências entre o contrato e seus anexos, prevalecerá o disposto neste contrato.

2.3 Se a divergência for entre anexos, prevalecerá aquele de data mais recente.

2.4 No caso de divergência entre os anexos e a Proposta da CONTRATADA prevalecerão os documentos da CPTM.

3 EXECUÇÃO DOS SERVIÇOS

3.1 Os serviços deverão ser executados, estritamente em conformidade com as condições pormenorizadamente definidas e especificadas neste contrato e seus anexos, partes integrantes deste instrumento para todos os fins e efeitos legais.

4 PRAZO DE EXECUÇÃO DOS SERVIÇOS E DE VIGÊNCIA

4.1 O presente Contrato entra em vigor na data de sua assinatura.

4.2 O prazo de execução dos serviços é de 30 (trinta) meses, a contar da data de início estabelecida na Ordem de Serviço - O.S., a ser emitida pela CPTM em até 15 (quinze) dias corridos, da data da assinatura do contrato.

4.3 O prazo referido acima poderá ser prorrogado, até o limite de 60 (sessenta) meses, mediante acordo entre as partes e deverão ser feitos por meio de termos de aditamento, mantidos os preços unitários e demais condições contratuais.

4.4 A inobservância do prazo de execução estipulado nesta cláusula somente será admitida pela CPTM, quando fundamentada nos motivos de força maior, nos termos do artigo 393, do Código Civil Brasileiro, ou por motivos imputáveis à CPTM, os quais deverão ser comprovados sob pena de a CONTRATADA incorrer nas penalidades estipuladas neste contrato.

4.5 A hipótese de que trata o subitem anterior somente será considerada mediante solicitação escrita e fundamentada da CONTRATADA, no prazo máximo de 10 (dez) dias corridos contados da ocorrência do fato gerador do atraso e desde que aceita, também por escrito, pela CPTM.

4.6 Na contagem dos prazos estabelecidos neste contrato, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.7 Só se iniciam e vencem os prazos referidos neste contrato em dia de expediente na CPTM.

5 VALOR DO CONTRATO

5.1 As partes atribuem a este contrato, para efeitos de direito, o valor total de R$ 54.822.367,80 (cinquenta e quatro milhões, oitocentos e vinte e dois mil, trezentos e sessenta e sete reais e

oitenta centavos), em julho/2025.

5.1.1 O valor definido nesta cláusula contempla todos os equipamentos, materiais, instrumentos, transportes, mão-de-obra, acessórios, seguros cabíveis, pessoal, bem como os custos indiretos (impostos, tributos, encargos, taxas, emolumentos, etc.) e outras despesas, de modo a constituir a única contraprestação pela execução dos serviços objeto deste contrato.

6 DOTAÇÃO ORÇAMENTÁRIA

6.1 A despesa referente ao valor do presente contrato será processada por conta de recursos que estão alocados no Programa de Trabalho: 26783370746270000 - Natureza de Despesa: 339040 - Origem dos Recursos: 150140004 - RAV n° 6560/2025.

7 REGIME DE EXECUÇÃO

7.1 Os serviços objeto do presente contrato serão executados sob o regime de empreitada por preço global.

8 MEDIÇÃO

8.1 Os serviços objeto deste contrato serão apontados por medições mensais e entrega dos correspondentes relatórios, após a realização dos mesmos, conforme Cronograma Físico-Financeiro e Termo de Referência, partes integrantes do presente instrumento.

8.2 A medição será realizada diretamente pela CONTRATADA, indicando as quantidades correspondentes aos serviços previstos e realizados, a data e o local onde os mesmos foram executados, o valor correspondente as atividades executadas no período abrangido pela mesma constando, também, os serviços acumulados, bem como o saldo, sempre respeitando o Cronograma Físico-Financeiro – Anexo 3.

8.3 A medição deverá ser numerada sequencialmente, discriminando o número deste contrato, o seu objeto e a Ordem de Serviço correspondente.

8.4 A medição deverá ser apresentada à CPTM até o 5º (quinto) dia útil, contado do último dia do período de adimplemento de cada parcela, mediante protocolo onde conste a data de sua entrega.

8.5 A CPTM terá o prazo de 5 (cinco) dias úteis para a conferência da medição e dos relatórios e a sua aprovação.

8.6 A medição não aprovada pela CPTM será devolvida à CONTRATADA para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido no subitem anterior, a partir da data de sua reapresentação para nova conferência.

8.7 A parcela não rejeitada seguirá o processamento normal, conforme estabelecido nesta cláusula.

8.8 A devolução da medição não aprovada pela CPTM em hipótese alguma servirá de pretexto para que a CONTRATADA suspenda a execução dos serviços.

8.9 Na hipótese de devolução da medição de forma indevida, a CPTM ressarcirá à CONTRATADA o valor da rejeição, acrescido de juros moratórios de 6% (seis por cento) ao ano, calculados “pro rata tempore” desde a data de vencimento original até a do efetivo pagamento.

9 CONDIÇÕES DE PAGAMENTO

9.1 A CPTM procederá ao pagamento nas condições previstas nesta cláusula.

9.1.1 Após a aprovação da medição e do recebimento da respectiva Carta de Aprovação de Faturamento - CA, a CONTRATADA deverá, no prazo de até 02 (dois) dias úteis, apresentar ao Departamento Fiscal – DFSF da CPTM, via endereço eletrônico DFSF-NRDF@cptm.sp.gov.br, o (s) documento(s) fiscal (is) pertinentes à operação, dos quais deverão constar todos os tributos incidentes na fonte sobre a prestação dos serviços, conforme estabelecido na cláusula de tributos deste contrato.

9.1.2 Na nota fiscal e no documento fiscal deverão ainda ser indicados o número do contrato, o período medido, o número da Ordem de Serviço, o número da medição e os locais de realização dos serviços. No processamento do pagamento, obedecerá a CPTM as disposições contidas na Lei nº 8.212, de 24 de julho de 1991, regulamentada pelo Decreto n° 3.048, de 06 de maio de 1999, e normas complementares.

9.1.3 O documento fiscal não aprovado pela CPTM será devolvido à CONTRATADA para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido no subitem 9.1.1, a partir da data de sua reapresentação.

9.1.4 A devolução do documento fiscal não aprovado pela CPTM em hipótese alguma servirá de pretexto para que a CONTRATADA suspenda a execução dos serviços.

9.1.5 A CPTM efetuará o pagamento no prazo de 30 (trinta) dias corridos, a contar da entrega da nota fiscal de cada parcela no DFSF, desde que aprovados a medição, a nota fiscal e o documento fiscal, nos prazos estabelecidos nas cláusulas da medição e de pagamento deste contrato.

9.1.5.1 A efetivação do(s) pagamento(s) oriundo(s) deste contrato, fica condicionada à inexistência de registro da CONTRATADA no CADIN Estadual, nos termos da Lei nº 12.799, de 11 de janeiro de 2008.

9.1.6 Na hipótese de ocorrer devolução da medição, conforme estabelecido na correspondente cláusula deste contrato, o prazo de pagamento se dilatará pelo número de dias corridos contados entre a data de devolução e a(s) data(s) da nova apresentação.

9.1.7 Caso ocorra atraso no pagamento, por motivos imputáveis à CPTM, os valores devidos serão acrescidos de juros moratórios de 6% (seis por cento) ao ano, calculados “pro rata tempore", desde a data de vencimento da obrigação até a do efetivo pagamento, conforme fórmula abaixo:

$VJM = VA \times (1,06)^{n/365}$, onde:

VJM = Valor em atraso acrescido de juros moratórios
VA = Valor em atraso
n = Número de dias corridos em atraso

9.1.8 Excetuam-se os atrasos decorrentes de caso fortuito ou de força maior previstos no artigo 393, do Código Civil Brasileiro, desde que devidamente comprovados.

9.1.9 Os valores de eventuais reajustamentos de preços deverão ser indicados no corpo do documento de cobrança e faturados no mesmo documento fiscal, porém em separado do valor principal, acompanhados da respectiva memória de cálculo.

9.1.10 O pagamento deverá ser efetuado no Sistema de Administração Financeira de Estados e Municípios – SIAFEM através de transferência de Unidade Gestora no prazo de 30 (trinta) dias em obediência ao Decreto nº 43.914 de 26/03/1999, contados da data da entrega da nota fiscal/fatura.

9.1.11 A CPTM poderá, sem prejuízo das penalidades cabíveis, descontar dos pagamentos das faturas, importâncias que, a qualquer título, forem devidas pela CONTRATADA em razão do presente contrato.

9.1.12 Quaisquer títulos de cobrança emitidos pela CONTRATADA contra a CPTM não poderão ser negociados e deverão ser mantidos em carteira. A CPTM não se obriga a efetuar pagamentos de títulos colocados em cobrança por meio de Bancos ou empresas de "factoring".

9.1.13 A CONTRATADA dará como quitadas todas as duplicatas ou outros documentos de cobrança sacados contra a CPTM, pela efetivação do pagamento por meio da transferência de Unidade Gestora.

10 REAJUSTAMENTO DE PREÇOS

10.1 Para o reajustamento dos preços contratados, deverá ser observada a legislação vigente, mediante a aplicação da seguinte fórmula:

$$R = P0.(\frac{A1}{A0} - 1)$$

Onde:

Variável	Valor	Descrição
R	-	Parcela de Reajuste
P0	-	Preço na data base de referência do contrato
A0,A1	-	Variação referente ao mês Base (A0) e o mês de aplicação do Reajuste (A1): IPC-FIPE-Categoria GERAL

10.2 A periodicidade anual para a aplicação do reajuste será contada a partir do mês base dos preços – julho/2025.

10.3 Na hipótese de até a emissão do documento de cobrança, não ter sido divulgada a variação do índice, o reajustamento será calculado, de forma provisória, por meio da aplicação do último índice conhecido.

10.4 Quando da publicação do índice definitivo, a CONTRATADA deverá emitir nota fiscal e documento de cobrança referentes à diferença do reajuste, cujo pagamento deverá ocorrer a 10 (dez) dias corridos da entrega desses documentos à CPTM ou na data de vencimento original, o que ocorrer depois.

10.5 Na hipótese de vir a ser editada legislação conflitante com o quanto disposto nesta cláusula, as partes concordam desde já com a sua adequação aos dispositivos legais pertinentes.

10.6 Na hipótese de ocorrer atraso em relação ao previsto no cronograma contratual, por motivos imputáveis à CONTRATADA, o reajuste referente à parcela em atraso será calculado somente até a data em que os serviços deveriam ter sido executados pelo cronograma em questão.

11 TRIBUTOS

11.1 Todos os tributos e demais encargos devidos em decorrência, direta ou indireta, deste instrumento ou de sua execução, encontram-se incluídos no preço do contrato, competindo à CONTRATADA apurá-los e recolhê-los, sem direito a reembolso. Na hipótese de fornecimento que implique à CPTM apurar e recolher o ICMS – DIFERENCIAL DE ALÍQUOTA de que trata art. 117 do RICMS PAULISTA, a CONTRATADA desde logo autoriza que o pertinente valor seja deduzido/glosado de pagamentos subsequentes a ela efetuados.

11.2 A alíquota do ICMS, já inclusa no preço, será aquela vigente por ocasião do faturamento para a CPTM, correspondente ao respectivo Estado da Federação.

11.3 A CPTM se reserva o direito de solicitar à CONTRATADA, quando entender conveniente, a exibição dos comprovantes de recolhimento de tributos e demais encargos devidos, direta ou indiretamente, por conta deste instrumento.

11.4 Se durante o prazo de vigência deste contrato houver a alteração da alíquota dos tributos e demais encargos, ou a instituição de novos tributos que diretamente afetem os preços constantes deste contrato, os mesmos serão ajustados desde que devidamente comprovada a sua incidência e devidamente acordada entre as partes.

11.5 Caso haja majoração de tributos e esta esteja incluída na fatura, estando a CONTRATADA em atraso em relação ao Cronograma Físico-Financeiro, parte integrante deste instrumento, por fatos de sua exclusiva responsabilidade, a CPTM responderá, unicamente, pelo valor do tributo da época em que o evento deveria ter sido realizado, devendo a CONTRATADA suportar o ônus dessa diferença.

11.6 A CPTM, quando for a responsável tributária e nessa qualidade, apurará e reterá os tributos devidos dos pagamentos que efetuar e os recolherá segundo a legislação vigente.

11.7 As notas fiscais serão emitidas com observância do prazo de recolhimento dos tributos incidentes na fonte. Na hipótese de a emissão se der após o prazo de recolhimento ou de forma ou tempo que não permita o tempestivo recolhimento dos tributos incidentes na fonte, a CONTRATADA assume, desde logo, a responsabilidade pelo pagamento dos correspondentes encargos moratórios.

11.8 A CONTRATADA deverá fazer constar em suas notas fiscais todos os tributos incidentes na fonte, com indicação de sua base de cálculo, alíquota e do montante apurado. Na hipótese de isenção ou outra ocorrência que venha a inibir a incidência tributária, a CONTRATADA deverá indicá-la no documento fiscal, acompanhada do devido fundamento legal.

11.9 Na ocorrência de divergência entre o valor do tributo informado na nota fiscal e o efetivamente apurado, retido e recolhido na fonte, a CONTRATADA desde logo reconhece e autoriza à CPTM a deduzir a diferença apurada no próprio ou em futuros pagamentos a ela efetuados, a qualquer título.

11.10 Quando se tratar de faturamento decorrente de serviços tributados pelo Imposto sobre Serviços - ISS, a emissão dos devidos documentos fiscais obedecerá às normas legais aplicáveis. Na hipótese de serviços prestados em várias municipalidades e a legislação determinar o recolhimento do ISS para cada uma delas, a cobrança deverá ser efetuada por documentos

fiscais individualizados, de acordo com o município em que é prestado o serviço e para o qual deverá ser recolhido o imposto.

11.11 A CONTRATADA, se permitida a dedução de materiais da base de cálculo do ISS, deverá tomar as providências previstas na legislação municipal pertinente para que ocorra seu reconhecimento pelo órgão municipal competente, de modo a que o ISS indicado na nota fiscal corresponda exatamente ao valor a ser recolhido. Nestas providências incluem-se o prévio exame da fiscalização ou o cadastramento das notas fiscais de materiais em programas específicos de apuração de impostos municipais.

11.12 É de exclusiva responsabilidade da CONTRATADA quaisquer tributos e/ou encargos financeiros que venham a ser imputados a CPTM, em decorrência de incorreções de faturamento ou de situações que possam inibir a CPTM do cumprimento de suas obrigações tributárias, cabendo o respectivo ressarcimento.

12 OBRIGAÇÕES DA CPTM

12.1 A CPTM se responsabiliza por:

12.1.1 fornecer todas as informações necessárias e que estiverem disponíveis para o desenvolvimento dos serviços objeto do presente contrato;

12.1.2 notificar por escrito a CONTRATADA, fixando-lhe prazo para corrigir defeitos ou irregularidades encontrados na execução dos serviços;

12.1.3 fornecer todas as informações, completas e detalhadas, de todo o ambiente operacional de TI, incluindo: rede LAN e WAN, servidores, microcomputadores portáteis, microcomputadores desktop, terminais Thin Client, equipamentos de conectividade, links, softwares, sistemas aplicativos, sistemas de banco de dados, serviços de correio, impressão, WEB, Intranet, Internet, serviços relacionados à operação do ambiente de TI, além de informações de caráter institucional e organizacional da CPTM, necessárias ao pleno desenvolvimento dos serviços contratados;

12.1.4 notificar por escrito a CONTRATADA, da aplicação de eventual penalidade;

12.1.5 disponibilizar ambiente físico e infra-estrutura técnica adequados para instalação dos equipamentos e acomodação da equipe para prestação dos serviços;

12.1.6 disponibilizar estrutura de projetos (gerente de projeto, líder de projeto, principais key users funcionais, analistas de sistemas e analistas de negócios) adequados para suportar a execução do contrato;

12.1.7 viabilizar toda fiscalização necessária ao acompanhamento dos serviços;

12.1.8 promover o apontamento e aprovar a medição dos serviços executados, bem como efetuar os pagamentos devidos;

12.1.9 observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios da CONTRATADA, a que tenha acesso durante a execução do objeto deste Contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei Federal nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

13 OBRIGAÇÕES DA CONTRATADA

13.1 A CONTRATADA se obriga a:

13.1.1 preliminarmente ao início dos serviços, apresentar prova de inscrição no Cadastro dos Contribuintes Municipal expedida pelo Órgão competente da Prefeitura do Município onde está localizada a CONTRATADA, que demonstre a possibilidade de emissão das notas fiscais para os serviços ora contratados;

13.1.2 dar início à execução dos serviços a partir da data de início estabelecida na Ordem de Serviço – O.S. emitida pela CPTM;

13.1.3 disponibilizar quaisquer outros Softwares e/ou Sistemas Aplicativos, não constantes do Termo de Referência, necessários para a execução deste contrato;

13.1.4 disponibilizar telefonia móvel para os analistas, consultores e técnicos, objetivando o pleno desenvolvimento dos serviços contratados;

13.1.5 responsabilizar-se direta e exclusivamente pela execução do objeto deste contrato em plena conformidade com as disposições integrantes deste instrumento e, consequentemente, responder civil e criminalmente por todos os danos, perdas e prejuízos que venha a provocar ou causar, durante a execução dos serviços até o término do período de garantia e/ou até o prazo regido por legislação específica;

13.1.6 responsabilizar-se pela execução do objeto deste instrumento em plena conformidade com o Termo de Referência, a Proposta apresentada e demais anexos integrantes, bem como com as especificações e normas técnicas pertinentes, obrigando-se a reparar, refazer ou repor qualquer parte da execução dos serviços que venham a apresentar defeitos ou incorreções resultantes de vícios na execução, no prazo que lhe for fixado pela CPTM, sem ônus adicionais e sem prejuízo do disposto na cláusula de Penalidades;

13.1.7 responsabilizar-se pela composição do documento de faturamento, não podendo, portanto, no decorrer dos serviços, alterar a composição do faturamento descrita em sua planilha de proposta;

13.1.8 confiar os serviços a profissionais idôneos e habilitados, utilizando-se do mais alto nível da técnica atual;

13.1.9 comunicar, por escrito, a CPTM, caso venha a constatar, no decorrer da execução do objeto contratual, quaisquer discrepâncias, omissões ou erros, inclusive quaisquer transgressões às Normas Técnicas, regulamentos ou Leis em vigor, para que os mesmos sejam sanados;

13.1.10 responsabilizar-se tecnicamente pela direção e execução dos serviços objeto deste instrumento, conforme especificações técnicas e normas contratuais, e na forma da legislação em vigor;

13.1.11 executar os serviços dentro de padrões de qualidade e segurança que garantam o cumprimento do objeto contratual;

13.1.12 respeitar rigorosamente a legislação em vigor bem como cumprir as recomendações técnicas da CPTM relativas a execução do objeto deste contrato;

13.1.13 arcar com todos os impostos, taxas e contribuições incidentes sobre este contrato, efetuando os respectivos pagamentos na forma e nos prazos determinados por

lei;

13.1.14 zelar no que lhe compete, pelo correto encaminhamento das medições, faturas e demais documentos decorrentes do presente contrato, nos endereços e aos destinatários indicados pela CPTM, de forma a evitar extravios que possam implicar morosidade ou até suspensão nos compromissos e obrigações por parte da CPTM;

13.1.15 manter, por seus dirigentes, empregados, prepostos ou representantes a qualquer título, sigilo a respeito das informações a que tiver acesso em decorrência deste contrato, incluindo as relativas a relatórios técnicos e procedimentos operacionais, sendo vedada a utilização das informações sigilosas para outro fim que não a normal execução deste contrato e a manutenção dos registros e arquivos exigidos pela legislação;

13.1.16 acatar no prazo de 24 (vinte e quatro) horas as modificações sugeridas pelos Fiscais da CPTM em relação a procedimentos técnicos adotados nos serviços, à observância das normas técnicas e de segurança;

13.1.17 responsabilizar-se pelo estudo de todos os documentos e outros elementos fornecidos pela CPTM para a execução do objeto deste instrumento, não se admitindo, em nenhuma hipótese, a alegação de ignorância dos mesmos;

13.1.18 substituir, em caso de solicitação da CPTM, o profissional alocado no contrato, em no máximo 5 (cinco) dias úteis a partir da solicitação;

13.1.19 manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação exigidas na Dispensa de Licitação que deu origem ao presente instrumento;

13.1.20 acompanhar e fornecer, durante a fase de transição ao final do contrato, todas as informações necessárias ao pleno conhecimento do futuro fornecedor acerca do ambiente de TI da CPTM;

13.1.21 no prazo máximo de 20 dias da assinatura deste instrumento, a CONTRATADA deverá:

a) mobilizar equipe com conhecimento técnico, experiência e em quantidades adequadas para a absorção do conhecimento de todo o ambiente de TI da CPTM, incluindo suas conexões com outras entidades governamentais e prestadores de serviços.

b) acompanhar o fornecedor atual, buscando de forma pró-ativa todas as informações necessárias para complementar o conhecimento obtido.

c) operar todo o ambiente da CPTM, assistido pelo fornecedor atual. Para início desta etapa, a CONTRATADA deverá emitir declaração para a área de TI da CPTM, garantindo conhecer e ter pleno entendimento dos serviços a serem prestados, declarando-se apta a operá-los.

13.1.22 obedecer às normas e rotinas da CONTRATANTE, em especial as que disserem respeito à proteção de dados pessoais, à segurança, à guarda, à manutenção e à integridade das informações coletadas, custodiadas, produzidas, recebidas, classificadas, utilizadas, acessadas, reproduzidas, transmitidas, distribuídas, processadas, arquivadas, eliminadas ou avaliadas durante a execução do objeto, observando as normas legais e regulamentares aplicáveis;

13.1.23 guardar confidencialidade no uso das informações ou documentos de qualquer natureza de que venha a tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização e custódia.

14 FISCALIZAÇÃO

14.1 A CPTM reserva-se o direito de exercer diretamente por si ou por intermédio de terceiros, devidamente credenciados, ampla fiscalização do cumprimento das obrigações atribuídas à CONTRATADA, solicitando à mesma, sempre que achar conveniente, informações do seu andamento, devendo esta prestar os esclarecimentos desejados, bem como comunicar à CPTM quaisquer fatos ou anormalidades que porventura possam prejudicar o bom andamento ou o resultado final dos serviços contratados.

14.2 No desempenho de suas atividades, é assegurado à fiscalização o direito de verificar a perfeita execução do presente ajuste em todos os termos e condições.

14.3 A ação ou omissão total ou parcial da fiscalização não eximirá a CONTRATADA de total responsabilidade de executar os serviços, com toda cautela, boa técnica e qualidade dos serviços contratados.

14.4 A CONTRATADA obriga-se a atender as determinações da fiscalização da CPTM relativas à técnica de execução e à segurança do trabalho.

14.5 Todos os trabalhos serão verificados pelo Gestor do Contrato antes de serem apropriados, cabendo à CONTRATADA tomar todas as providências necessárias para essa verificação, a qual será realizada com base nas Especificações e Normas Técnicas pertinentes.

14.6 Até o recebimento definitivo do objeto do contrato/serviço, a CONTRATADA será responsável, sem qualquer ônus para a CPTM, pela conservação e manutenção dos serviços por ela executados.

15 PENALIDADES

15.1 Salvo ocorrência de casos fortuitos ou de força maior, devida e formalmente justificados / comprovados, ao não cumprimento, por parte da CONTRATADA, das obrigações assumidas, ou a infringência de preceitos legais pertinentes, poderão ser aplicadas, segundo a gravidade da falta e observada a dosimetria do artigo 257 do Regulamento de Licitações, Contratos e demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023, garantida prévia defesa, no prazo de 10 (dez) dias úteis, as seguintes penalidades:

15.1.1 a CONTRATADA compromete-se com determinados *SLAs* (*Service Level Agreement*) mínimos e o seu não cumprimento nos prazos acordados submete a CONTRATADA às penalidades indicadas no quadro seguinte:

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
Coordenação de Operação de TI e Projetos	Sugestões de melhoria implementadas	Mínimo de 1 por trimestre	Trimestral	Penalidade de 0,01% no valor do contrato	Relatório de melhorias implementadas após aprovação da CPTM
	Relatório de gestão de problemas	95% em até 10 dias úteis da data de identificação do problema	Mensal	Penalidade de 1% no pagamento	Relatório de gestão e acompanhamento dos problemas, relatório de

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
				mensal da medição.	causa raiz do problema e controle de erros.
	Relatório de gestão de capacidade	Consumo de acima 80% dos recursos até 180 dias úteis antes do esgotamento	Mensal	Penalidade de 1% no pagamento mensal da medição.	Relatório de consumo, otimização de recursos e previsão de esgotamento com análise e parecer dos especialistas técnicos.
	Relatório de Gestão de ativos	98% dos ativos gerenciados na ferramenta de ITSM	Mensal	Penalidade de 1% no pagamento mensal da medição.	Relatório de gestão, identificação, localização, utilização e ciclo de vida (Hardware, Software)
	Relatório de Gestão dos itens de configuração	98% dos ativos gerenciados na ferramenta de ITSM	Mensal	Penalidade de 1% no pagamento mensal da medição.	Relatório de gerenciamento dos itens de configuração e seus relacionamentos para entrega de cada serviço.
	Catálogo de serviços gerenciado e atualizado	99,5% do catálogo gerenciado e atualizado	Trimestral	Penalidade de 0,1% no valor do contrato	Apresentação do catálogo de serviço com as melhorias implementadas
	Habilitação de Mudanças	84,5% realizadas com sucesso dentro da Janela Operacional, incluindo rollback	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de mudanças executadas
Monitoramento de Ambiente de TI (NOC)	Detecção preventiva de incidentes	95% dos incidentes críticos identificados antes da indisponibilidade. Não aplicável a links	Mensal	Penalidade de 2% no pagamento mensal do serviço	Relatório de incidentes, dashboard de monitoramento
	Tempo de resposta a incidentes críticos (início do atendimento, excluindo resolução)	< 30 minutos	Mensal	Penalidade de 1% no pagamento mensal do serviço por SLA Violado	Relatório mensal com Logs de monitoramento, atendimento e resposta
	Disponibilidade do ambiente crítico (Serviços críticos e infraestrutura) desconsiderando situações de falha de hardware	98%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de disponibilidade de serviços e infraestrutura
Gestão e Operação do Ambiente de Rede	Disponibilidade do ambiente de rede, desconsiderando situações de falha de hardware	98%	Mensal	Penalidade de 2% no pagamento mensal do serviço	Relatório de disponibilidade, desempenho e otimização

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
	Tempo de resolução de falhas de criticidade alta em até 4 horas	80%	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade média em até 8 horas	80%	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade baixa em até 24 horas úteis	90%	Mensal	Penalidade de 0,5% no pagamento mensal do serviço	Relatório de incidentes
Administração e Operação de Banco de Dados	Disponibilidade dos Sistemas Gerenciadores de Banco de dados (SGBD)	98%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de disponibilidade, desempenho e otimização
	Tempo de resolução de falhas de criticidade alta em até 4 horas. Excluindo chamados que envolvam a Oracle para resolução.	80%	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade média em até 8 horas. Excluindo chamados que envolvam a Oracle para resolução	80%	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade baixa em até 24 horas. Excluindo chamados que envolvam a Oracle para resolução	90%	Mensal	Penalidade de 0,5% no pagamento mensal do serviço	Relatório de incidentes
Gestão e Operação do	Disponibilidade da plataforma VMware	98%	Mensal	Redução de 2% no pagamento mensal	Relatório de disponibilidade de VMs, desempenho e otimização

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
Ambiente Virtualizado					
	Tempo de resolução de falhas de criticidade alta em até 4 horas	80%	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade média em até 8 horas	80%	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade baixa em até 24 horas úteis	90%	Mensal	Penalidade de 0,5% no pagamento mensal do serviço	Relatório de incidentes
Gestão e Operação de Soluções de Armazenamento	Disponibilidade das soluções de armazenamento (storage e file server)	98%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de disponibilidade, desempenho e otimização
	Tempo de resolução de falhas de criticidade alta em até 4 horas	80%	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade média em até 8 horas	80%	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de incidentes
	Tempo de resolução de falhas de criticidade baixa em até 24 horas úteis	90%	Mensal	Penalidade de 0,5% no pagamento mensal do serviço	Relatório de incidentes
Gestão e Operação de Backup	Conformidade com a Política de Backup	99% das rotinas concluídas conforme programado	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de backup, restauração e otimização
	Tempo de restauração de backup	99% das rotinas concluídas conforme solicitado	Mensal	Penalidade de 1% no pagamento mensal do serviço	Logs de restauração de backup
Gestão e operação de segurança cibernética	Início de atendimento para incidentes de segurança	< 2 horas	Mensal	Penalidade de 1% no pagamento mensal do	Relatório de incidentes de segurança

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
				serviço por incidente	
	Relatório de gestão de segurança	95% dos eventos registrados e apresentados.	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de segurança cibernética contemplando as soluções de firewall e solução estendida contendo: Visão geral dos incidentes de segurança, discriminação dos tipos de incidentes com os detalhes técnicos dos incidentes detectados, top ameaças analisadas, top hosts infectados, recomendações de segurança, estatísticas do tráfego analisado, conexões VPN realizadas, bloqueios de tráfego malicioso detectados e prevenidos e indicadores de risco e vulnerabilidades do ambiente.
Solução de Firewall	Disponibilidade da Plataforma de Firewall fornecida como serviço	98%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de firewall de borda, VPN, IDS/IPS e filtro de Conteúdo
	Disponibilidade da plataforma firewall existente na contratada	98%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de firewall de borda, VPN, IDS/IPS e filtro de Conteúdo
	Gestão de regras e políticas de segurança	até 8 horas úteis	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de solicitações
Solução estendida de detecção e resposta, segurança de endpoints e rede	Antivírus para estações de trabalho no domínio	95% do parque protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos
	Antivírus para servidores	99% do parque protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos
	Ativos fora da rede	80% protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
	Identificação e correlação automática de eventos suspeitos em múltiplos vetores (endpoints, rede, servidores, cloud, firewall).	95% identificado e correlacionado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade.
	Análise automática do tráfego e detecção de comportamentos anômalos.	95% analisado e tratado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade.
	Relatórios de conformidade	95% sob demanda	Mensal	Penalidade de 1% no pagamento mensal do serviço	Geração de Dashboards e exportação de dados para auditoria e conformidade (ISO 27001, NIST).
	Detecção baseada em IA de desvios comportamentais de usuários e dispositivos.	95% analisado e tratado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade.
	Relatório de Vulnerabilidades	90% das vulnerabilidades identificadas	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de detecção, priorização e acompanhamento de vulnerabilidades conforme MITRE ATT&CK com recomendações de segurança e tratamento.
	Execução de playbooks de resposta automática a incidentes.	95% de eficácia nas regras de automação configuradas	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de incidentes e automações realizadas

15.2 As multas serão aplicadas mensalmente e sua totalidade não poderá exceder o limite de 30% do valor do contrato, conforme § 2º do Artigo 247 do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

15.3 Suspensão temporária de participação em licitação e impedimento de contratar com a CPTM, por prazo não superior a 24 (vinte e quatro) meses, nos termos do Artigo 247, inciso III do Regulamento de Licitações, Contratos e demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023, sem prejuízo das multas previstas no contrato e das demais cominações legais.

15.4 As penalidades de multa serão, sempre que possível, descontadas dos créditos da CONTRATADA ou, se for o caso, cobradas administrativa ou judicialmente.

15.5 O pagamento das multas compensatórias não exime a CONTRATADA da reparação dos eventuais danos, perdas ou prejuízos que ultrapassem o valor das penalidades aplicadas, devendo ser adotado o procedimento do artigo 248 do Regulamento de Licitações, Contratos e demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

15.6 Na hipótese de não existirem pagamentos previstos efetivamente configurados, a CONTRATADA deverá efetuar a quitação da multa em até 48 (quarenta e oito) horas contadas do recebimento do documento de cobrança respectivo, no Departamento de Finanças da CPTM, sob pena de, em não o fazendo, sujeitar-se aos procedimentos judiciais cabíveis.

15.7 O não pagamento da multa no prazo estipulado importará na incidência de juros moratórios de 6% (seis por cento) ao ano “pro rata tempore”, até seu efetivo pagamento, utilizando-se para o cálculo a mesma fórmula indicada na cláusula de pagamento deste contrato.

15.8 O processo administrativo não será instaurado quando os motivos forem de responsabilidade da CPTM.

15.9 Se em qualquer momento no curso da execução deste contrato, a CONTRATADA encontrar-se numa situação que a impeça de proceder o serviço ou cumprir algum compromisso, a mesma deverá notificar a CPTM por escrito, em um prazo não superior a 30 (trinta) dias a partir da ocorrência, informando o atraso, sua duração estimada e suas causas. Depois de receber a notificação, a CPTM avaliará a situação e poderá, a seu critério, prorrogar o prazo outorgado à CONTRATADA para o cumprimento dos serviços ou dos compromissos. Neste caso, a prorrogação será ratificada pelas partes mediante formalização do competente instrumento de aditamento.

16 RESCISÃO

16.1 Constituem motivos para rescisão do contrato:

a) o não cumprimento ou cumprimento irregular de cláusulas contratuais, especificações, projetos ou prazos;

b) a lentidão do seu cumprimento, levando a CPTM a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

c) a subcontratação do objeto que importe em desatendimento das condições de qualificação técnica e sem prévia autorização da CPTM;

d) a fusão, cisão, incorporação, associação da CONTRATADA com outrem, bem como a cessão ou transferência, total ou parcial, sem prévia autorização da CPTM para avaliação da manutenção das condições de habilitação, contratação e eventual prejuízo à execução do objeto contratado;

e) o desatendimento das determinações regulares do gestor ou fiscal do contrato, assim como as de seus superiores;

f) o cometimento reiterado de faltas na execução contratual;

g) a dissolução da sociedade, o falecimento do contratado, a decretação de falência ou a insolvência civil do contratado;

h) a alteração social ou a modificação da finalidade ou da estrutura da CONTRATADA que prejudique a execução do contrato;

i) razões de interesse público, justificadas e determinadas pela Diretoria Colegiada;

j) o descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação ou de contratação pela CONTRATADA;

k) 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;

l) a prática de atos lesivos à CPTM previstos na Lei Federal nº 12.846/2013.

16.2 Constituem motivos para rescisão do contrato, mediante denúncia da CONTRATADA:

a) suspensão de execução do contrato, por ordem escrita da CPTM, por prazo superior a 3 (três) meses;

b) repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;

c) atraso superior a 2 (dois) meses, contado da emissão da nota fiscal, dos pagamentos ou de parcelas de pagamentos devidos pela CPTM por despesas de obras, serviços ou fornecimentos.

16.3 A rescisão por iniciativa da CONTRATADA, deverá ser precedida de comunicação escrita e fundamentada, com antecedência mínima de 60 (sessenta) dias.

16.4 Em qualquer hipótese de rescisão contratual, os serviços já elaborados ou em elaboração, pela CONTRATADA, até a data rescisória, passarão à propriedade da CPTM.

16.5 A rescisão consensual ocorrerá por acordo entre as partes, mediante autorização escrita e fundamentada da autoridade competente, e será reduzida a termo no processo respectivo, desde que haja conveniência para a CPTM.

16.6 Quando a rescisão ocorrer sem que haja culpa da outra parte contratante, será esta ressarcida dos prejuízos que houver sofrido, nos termos do disposto no artigo 187, do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

16.7 As hipóteses de extinção a que se referem as alíneas “a”, “b” e “c” do subitem 16.2 acima observarão as seguintes disposições:

a) não serão admitidas em caso de calamidade pública, de grave perturbação da ordem interna ou de guerra, bem como quando decorrerem de ato ou fato que o contratado tenha praticado, do qual tenha participado ou para o qual tenha contribuído;

b) assegurarão ao contratado o direito de optar pela suspensão do cumprimento das obrigações assumidas até a normalização da situação.

16.8 Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa, observando-se o procedimento previsto no artigo 189 do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

17 SUBCONTRATAÇÃO

17.1 Toda e qualquer subcontratação relativa ao presente contrato ficará limitada às atividades acessórias e complementares e deverá ser previamente apresentada para aprovação da CPTM, podendo esta autorizar ou não a proposta. A autorização da CPTM não desobriga a CONTRATADA da integral responsabilidade pela subcontratação e pelos correspondentes serviços e/ou fornecimentos realizados. Na solicitação de autorização da subcontratação, será informado e detalhado pela CONTRATADA o serviço ou o material a ser subcontratado e as condições de execução dos mesmos. Sendo autorizada a subcontratação pela CPTM, o subcontratado deverá submeter-se às normas por ela estabelecidas, bem como às cláusulas e condições deste instrumento.

17.2 Mesmo ocorrendo a subcontratação, a CONTRATADA será a única e exclusiva responsável, pelos termos deste instrumento, perante a CPTM, órgãos e entidades públicas e privadas e terceiros e será a única a emitir faturamento contra a CPTM.

17.3 A CPTM deverá ter acesso liberado, pela CONTRATADA, à todas as subcontratadas e/ou seus fornecedores de materiais e equipamentos.

17.4 Na hipótese de não aprovação do serviço de subcontratação, a CONTRATADA deverá apresentar novo subcontratado para o mesmo escopo, não cabendo à CPTM qualquer responsabilidade de eventual comprometimento do objeto deste instrumento.

18 GARANTIA TÉCNICA

18.1 A CONTRATADA deverá garantir, em razão da sua responsabilidade técnica, a correção e/ou substituição, sem custo adicional para a CPTM, de quaisquer atividades desenvolvidas em desconformidade técnica ou diversa da especificada, devendo garantir ainda, a eficácia dos processos utilizados.

18.2 A CONTRATADA responderá pela qualidade dos serviços executados e demais documentos técnicos por ela desenvolvidos e apresentados, nos termos da legislação vigente aplicável à espécie.

18.3 Esta garantia deverá abranger todos e quaisquer tipos de falhas detectadas. Esta condição deverá ser observada, mesmo no caso de serviços executados, a qualquer tempo, pela CPTM ou por empresa especializada por ela contratada.

19 DIREITOS AUTORAIS

19.1 A CONTRATADA deverá garantir, indenizar e proteger a CPTM, seus sucessores, cessionários, clientes e usuários contra quaisquer responsabilidades, inclusive custos, indenizações, despesas, reclamações, ações ou processos judiciais sejam de que natureza forem, resultantes ou relacionados com qualquer infração dos dispositivos de marcas e patentes e/ou direitos autorais, com relação à execução do objeto deste contrato.

19.2 A CPTM comunicará à CONTRATADA, por escrito, quaisquer medidas judiciais ou extrajudiciais contra ela propostas, obrigando-se a CONTRATADA, conforme opção da CPTM, a:

19.2.1 defendê-la na forma entendida como a mais conveniente, pagando quaisquer danos, prejuízos e/ou custos a que venha a CPTM a ser condenada, por força das citadas medidas;

19.2.2 substituir, por produtos não infringentes, os produtos ou parte desses produtos declarados como tal, por decisão judicial, ou modificá-los, de forma a torná-los produtos não infringentes; e

19.2.3 garantir à CPTM a continuidade e qualidade dos serviços previstos no contrato.

19.3 Em qualquer das três hipóteses, correrão por conta da CONTRATADA todas as despesas para adoção da opção entendida como mais conveniente pela CPTM, bem como as despesas relativas à consecução da(s) alternativa(s) indicada(s) e aprovada(s) pela CPTM.

19.4 Todos os sistemas e/ou programas de processamento de dados e seus aplicativos, implantados ou desenvolvidos pela CONTRATADA para a CPTM, são de propriedade da CPTM, não podendo ser reproduzidos ou copiados, cedidos ou transferidos, alugados ou vendidos, sem o prévio consentimento da CPTM, ressalvadas as disposições contidas na Resolução CC-52 de 23/06/2004. É facultado à CPTM registrar ou delegar a terceiros a responsabilidade de registro do software ou propriedade intelectual.

19.5 Os materiais e equipamentos a serem utilizados deverão encontrar-se totalmente desembaraçados de controle ou acordo com terceiros, especificamente patentes ou “know-how", que impeçam a CPTM o conhecimento de detalhes do projeto.

20 ALTERAÇÕES

20.1 O presente contrato poderá ser alterado, com as devidas justificativas, por acordo entre as partes, nos casos previstos no art. 173, do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

20.2 A CONTRATADA poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nos serviços, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

20.3 Nenhum acréscimo ou supressão poderá exceder o limite estabelecido no subitem anterior, salvo as supressões resultantes de acordo entre as partes, e deverão ser feitos por meio de termos de aditamento, mantidos os preços unitários e demais condições contratuais.

20.4 Os prazos de início de etapas de execução, de conclusão e de entrega, admitem prorrogações, se comprovadamente ocorrerem as circunstâncias descritas no artigo 177, do Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

20.5 Em caso de concessão de linhas ou serviços da CPTM, considerando o interesse público envolvido, a CPTM notificará a CONTRATADA com antecedência de 90 (noventa) dias, visando a desmobilização parcial ou total dos serviços previstos nesta contratação e/ou podendo realizar alterações no escopo em percentual superior a 25% (vinte e cinco por cento) ou mesmo antecipar o encerramento do contrato com a redução de escopo e de prazo, inclusive considerando o percentual acima estabelecido, a seu critério e sem custos adicionais de qualquer ordem às partes, renunciando, a CONTRATADA, expressamente e desde já, a qualquer direito ou valor a título de indenização e/ou reequilíbrio econômico-financeiro advindo dessa desmobilização, pois presumir-se-ão incorporados aos custos da proposta vencedora.

21 COMUNICAÇÕES

21.1 Todas as comunicações recíprocas, relativas a este contrato, serão consideradas como efetuadas se entregues por correspondências endereçadas como segue:

CPTM:
COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM
Rua Boa Vista nº 162, 6º andar - Centro

SÃO PAULO - SP
CEP 01014-902
CONTRATO DL00925-01 / PRODESP PD024401

CONTRATADA:
COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP
Rua Agueda Gonçalves nº 240 – Jardim Pedro Gonçalves
TABOÃO DA SERRA - SP
CEP 06760-900
CONTRATO DL00925-01 / PRODESP PD024401
CONTATO: Bruno Baranda / Luciano Benato / Rodrigo Gomes de Moura / Jobson Nunes de Souza
TEL: (11) 2868-3124 / (11) 2845-6000 / (11) 2845-6468 / (11) 2845-6344
E-MAIL: bruno.baranda@sp.gov.br / benato@sp.gov.br / rgmoura@sp.gov.br / jobson.souza@sp.gov.br

21.1.1 A entrega de qualquer correspondência, inclusive a que encaminha documentos ou Memorandos de Remessa - MR, será feita mediante correio eletrônico ou carta, ambos com comprovação de recebimento, que deverá ser juntado aos autos do processo de dispensa de licitação ou gestão. Em quaisquer dos casos, deverá sempre constar o número deste Contrato, o assunto, data de recebimento e o nome do remetente.

21.1.2 A CPTM e a CONTRATADA deverão, no prazo de 05 (cinco) dias úteis da assinatura deste instrumento, apresentar por escrito os nomes e respectivos cargos dos empregados designados pelas mesmas, para serem responsáveis pela gestão do presente contrato, aos cuidados dos quais deverão ser dirigidas as correspondências aqui previstas.

22 CONDIÇÕES DE RECEBIMENTO DO OBJETO DO CONTRATO

22.1 No recebimento e aceitação do objeto deste contrato serão observadas, no que couber, as disposições contidas no artigo 180, do Regulamento de Licitações, Contratos e demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

22.2 O objeto deste contrato será aceito pela CPTM, desde que atenda as condições estipuladas neste instrumento e nos documentos que fazem parte integrante do mesmo.

22.3 Os serviços serão recebidos provisoriamente, mediante a emissão de Termo de Recebimento Provisório - TRP, assinado pela CPTM, em até 15 (quinze) dias corridos da comunicação escrita de conclusão dos trabalhos pela CONTRATADA. Na emissão do TRP, deverão ser registradas todas as pendências a serem solucionadas no período de observação de defeitos ou falhas na conclusão do escopo. Não ocorrendo a solução das pendências nos prazos contratuais, a CONTRATADA passará à condição de inadimplência perante a CPTM.

22.4 O Recebimento Definitivo será efetuado no prazo de até 90 (noventa) dias corridos, contados da data de expedição do Termo de Recebimento Provisório - TRP, mediante a emissão do Termo de Recebimento Definitivo - TRD, assinado pela CPTM e pela CONTRATADA, desde que eliminadas as pendências quanto aos defeitos ou falhas na conclusão do escopo, consoante previsto no subitem 22.3.

23 DA PROTEÇÃO DE DADOS PESSOAIS

23.1 A CONTRATADA deve assegurar que o acesso aos dados pessoais compartilhados, seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados pertinentes, na medida em que sejam estritamente necessários para as finalidades deste Contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade, bem como à observância dos Códigos de Conduta e Integridade.

23.2 Nos casos em que a CONTRATADA receba da CPTM informações pessoais, estas devem ser utilizadas única e exclusivamente para a finalidade descrita no Contrato. Desta forma, salvo se expressamente autorizado, fica vedada a utilização de dados recebidos da CPTM para quaisquer fins não relacionados à efetiva prestação dos serviços deste Contrato, incluindo, mas não se limitando ao ganho financeiro a qualquer título com base em tais informações.

23.3 Considerando a natureza dos dados tratados, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos no *caput* do art. 6° da Lei Federal nº 13.709/2018, a CONTRATADA, garantirá, em relação aos dados pessoais, a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados e informações contra acessos não autorizados e prevenir a ocorrência de incidentes de segurança da informação, como também, de situações acidentais ou ilícitas de destruição, perda, alteração comunicação, difusão, deleção ou exposição indevida ou acidental de informações ou qualquer forma de tratamento inadequado ou ilícito.

23.4 Considerando a natureza do tratamento, a CONTRATADA deve, enquanto operadora de dados pessoais, implementar medidas técnicas, administrativas e organizacionais apropriadas para o cumprimento das obrigações da CPTM previstas na Lei Federal nº 13.709/2018.

23.5 A CONTRATADA deve, no que concerne aos dados pessoais compartilhados:

a) imediatamente notificar a CPTM ao receber requerimento de um titular de dados, na forma prevista no artigo 18 da Lei Federal nº 13.709/2018; e

b) sempre que solicitada, quando for o caso, prestar assistência e auxiliar a CPTM na elaboração da resposta à eventual requerimento visando o exercício de direitos por titulares de dados, garantidos pelo Capítulo III, da Lei Federal nº 13.709/2018 a que se refere o inciso I deste parágrafo.

23.6 A CONTRATADA deve notificar à CPTM, imediatamente, por meio do e-mail encarregado.dados@cptm.sp.gov.br a ocorrência de incidente de segurança relacionado a dados pessoais, fornecendo informações suficientes para que a CPTM cumpra quaisquer obrigações de comunicar à autoridade nacional e aos titulares dos dados a ocorrência do incidente de segurança sujeita à Lei Federal n° 13.709/2018.

23.7 Sem prejuízo da referida obrigação, a CONTRATADA deverá redigir um plano para resposta a incidentes de segurança, que deverá, minimamente, conter:

a) A referida comunicação, que, por sua vez, deverá conter, no mínimo:

b) (i) data e hora do incidente; (ii) data e hora da ciência pela CONTRATADA; (iii) relação dos tipos de dados afetados pelo incidente; (iv) número de usuários afetados (volumetria do incidente) e, se possível, a relação destes indivíduos; (v) dados de contato do Encarregado pela Proteção de Dados da CONTRATADA, ou pessoa por meio da qual seja possível obter informações sobre o ocorrido; e (vi) descrição das possíveis consequências do evento.

23.8 A seguir, e após autorização da CPTM, deverá a CONTRATADA providenciar:

a) A notificação dos indivíduos afetados, mediante texto previamente aprovado pela CPTM.

b) A notificação da Autoridade Nacional de Proteção de Dados, mediante texto previamente aprovado pela CPTM.

c) A adoção de um plano de ação que cesse e contemple os fatores que levaram à causa do incidente e aplique medidas que visem garantir a não recorrência deste evento.

23.9 Para os incidentes que envolvam Dados Pessoais causados em razão de conduta única e exclusiva da CONTRATADA, esta ficará responsável por adotar as medidas acima descritas, bem como adimplir com eventuais sanções determinadas pela Autoridade Nacional de Proteção de Dados.

23.10 Caso a CPTM assuma tais sanções, poderá exercer o direito de regresso perante a CONTRATADA, ficando este instrumento contratual constituído como título executivo extrajudicial.

23.11 Nos termos do parágrafo antecedente, a CONTRATADA deve adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança.

23.12 A CONTRATADA deve auxiliar a CPTM na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018, no âmbito da execução deste Contrato.

23.13 Na ocasião do encerramento deste Contrato, a CONTRATADA deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, devolver todos os dados pessoais à CPTM ou eliminá-los, conforme decisão da CPTM, inclusive eventuais cópias de dados pessoais tratados no âmbito deste Contrato, certificando por escrito, a CPTM, o cumprimento desta obrigação.

23.14 A CONTRATADA deve colocar à disposição da CPTM, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta cláusula, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pela CPTM ou auditor por ele indicado, em relação ao tratamento de dados pessoais.

23.15 Todas as notificações e comunicações realizadas nos termos desta cláusula devem se dar por escrito e ser entregues pessoalmente, encaminhadas pelo correio ou por e-mail para os endereços físicos ou eletrônicos informados em documento escrito emitido por ambas as partes por ocasião da assinatura do contrato, ou outro endereço informado em notificação posterior.

23.16 A CONTRATADA responderá por quaisquer danos, perdas ou prejuízos causados à CPTM ou a terceiros decorrentes do descumprimento da Lei Federal nº 13.709/2018 ou de instruções da CPTM relacionadas a este Contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização da CPTM em seu acompanhamento.

23.17 A CONTRATADA declara ciência de que a responsabilidade pela conformidade e observância à Lei Geral de Proteção de Dados Pessoais ou qualquer outra norma ou regulamento relacionado à privacidade e proteção de dados pessoais eventualmente aplicáveis (“Leis de Privacidade”), assim como as decisões quanto às atividades da empresa, no que tange ao tratamento de dados pessoais, competem única e exclusivamente à CONTRATADA, de modo que nem a CPTM e nem o Encarregado de Dados serão responsáveis por quaisquer danos, de qualquer ordem e natureza, tais como, e a estes não se limitando, indenizações, sanções administrativas, multas e outros que venham a ser, eventualmente, por ela suportados, em decorrência de infrações às Leis de Privacidade ou decisões inadequadas.

23.18 Nos termos do acima aduzido, caso algum terceiro demande, por qualquer meio, indenização ou sanção de qualquer natureza à CPTM, em decorrência da inobservância das Leis de Privacidade pela CONTRATADA, esta se obriga a assumir e/ou reembolsar os custos de defesa da CPTM e/ou do Encarregado de Dados, bem como indenizá-los por todos os prejuízos eventualmente suportados, incluindo os efeitos do artigo 125, inciso II, do Código de Processo Civil, comprometendo-se a CONTRATADA à aceitação da denunciação da lide.

23.19 Caso o objeto da presente contratação envolva o tratamento de dados pessoais com fundamento no consentimento do titular de que trata o inciso I dos artigos 7º e 11ª da Lei nº 13.709/2018, deverão ser observadas pela CONTRATADA ao longo de toda a vigência do contrato todas as obrigações específicas vinculadas a essas hipóteses legais de tratamento de dados pessoais, conforme instruções por escrito da CPTM.

23.20 É vedada a transferência de dados pessoais, pela CONTRATADA, para fora do território do Brasil sem o prévio consentimento, por escrito, da CPTM, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

23.21 A CONTRATADA não poderá realizar subcontratação, tampouco divulgar/compartilhar dados pessoais a qualquer subcontratado, ou substituir subcontratado, exceto se previamente autorizada de forma específica e por escrito pela CPTM.

23.22 A CONTRATADA deve tomar medidas razoáveis para assegurar que empregados, prepostos ou colaboradores de qualquer subcontratado que necessitem conhecer/acessar dados pessoais relacionados à execução deste contrato estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade, e cumprir, no tocante à subcontratação todas as disposições aplicáveis da Lei Federal nº 13.709/2018.

23.23 A subcontratação, mesmo quando autorizada pela CPTM, não exime a CONTRATADA das obrigações decorrentes deste contrato, de modo que a CONTRATADA permanecerá por elas integralmente responsável perante a CPTM, inclusive na hipótese de descumprimento dessas obrigações por subcontratada.

24 NOVAÇÃO

24.1 Se qualquer das partes contratantes permitir, por tolerância, o descumprimento, no todo ou em parte, de qualquer das cláusulas ou condições do presente instrumento ou de seus anexos, tal fato não implicará novação das obrigações ora assumidas.

25 LEGISLAÇÃO APLICÁVEL

25.1 Aplica-se a este contrato, e principalmente aos casos omissos, o disposto na Lei Federal n° 13.303, de 30 de junho de 2016 e no Regulamento de Licitações, Contratos e Demais Ajustes da Companhia Paulista de Trens Metropolitanos - CPTM - Vigente a partir de 04/12/2023.

26 **VÍNCULO**

26.1 O presente contrato está vinculado ao Processo DL00925 e à proposta da CONTRATADA.

27 FORO

27.1 As partes signatárias deste instrumento elegem, com exclusão de qualquer outro, por mais privilegiado que seja, o Foro Central da Comarca da Cidade de São Paulo para dirimir quaisquer litígios referentes a este Contrato.

E, por estarem, assim, justas e contratadas, firmam as partes o presente instrumento na presença das testemunhas abaixo, para que produza os efeitos legais.

Pela **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM**:

ANA CAROLINE DE FARIA EDUARDO BORGES
Diretora Administrativa e Financeira
ana.borges@cptm.sp.gov.br
e-mail pessoal: N/I
CPF nº 003.938.371-73
RG nº 4.296.749

MICHAEL SOTELO CERQUEIRA
Diretor Presidente
michael.cerqueira@cptm.sp.gov.br
e-mail pessoal: N/I
CPF nº 284.295.458-08
RG nº 33.427.569-6

GEAN LIMA FERREIRA
Gerente de Tecnologia da Informação
gean.ferreira@cptm.sp.gov.br
E-mail pessoal: N/I
CPF nº 270.806.028-74
RG nº 28.302.367-3

Pela **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**

GILENO GURJÃO BARRETO
Diretor Presidente
gileno.barreto@sp.gov.br
e-mail pessoal: N/I
CPF nº 315.099.595-72
RG nº 842.620 SSP-SE

THIAGO WALTZ ALVES
Diretor Comercial
thiago.waltz@sp.gov.br
e-mail pessoal: N/I
CPF nº 950.082.761-15
RG nº 1.855.322 SSP-DF

TESTEMUNHAS:

MARIANA MIDORI KAWANO
Analista de Processos de Contratação

KATIA INFANTE NATO
Assessora Executiva

Documento assinado eletronicamente por **Gean Lima Ferreira**, **Gerente**, em 11/11/2025, às 14:37, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Michael Sotelo Cerqueira**, **Diretor Presidente**, em 11/11/2025, às 18:53, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 12/11/2025, às 16:31, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 12/11/2025, às 18:35, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Mariana Midori Kawano**, **ANL De Processos De Contratacao**, em 13/11/2025, às 09:08, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Katia Infante Nato**, **Assessor Executivo**, em 13/11/2025, às 09:09, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Ana Caroline De Faria Eduardo Borges**, **Diretor**, em 13/11/2025, às 09:18, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0088900077** e o código CRC **2118B141**.

ANEXO 1

CONTRATO DL00925-01 / PRODESP PD024401

TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA

TR.DFIO.002/2025

OBJETO: PRESTAÇÃO DE SERVIÇOS CONTINUADOS, ESPECIALIZADOS EM TI - TECNOLOGIA DA INFORMAÇÃO, QUE SE CONSTITUEM DE UMA SOLUÇÃO GLOBAL AO AMBIENTE DE TI E DE SEGURANÇA CIBERNÉTICA.

Conteúdo

1. DESCRIÇÃO DO AMBIENTE DE TI

O ambiente de TI – Tecnologia da Informação da CPTM está baseado em uma rede MAN, rede local de microcomputadores com servidores padrão CISC, processando aplicações corporativas gerais e de uso departamental, desenvolvidas internamente ou mesmo aplicações de terceiros, todos utilizando ou banco de dados Oracle ou Microsoft SQL Server.

As comunicações entre as unidades administrativas (sites) Presidente Altino, Lapa, Barra Funda, Luz e Brás estão conectadas por um backbone gigabit (topologia estrela), onde o nó central está localizado no site Brás. A unidade administrativa Boa Vista está interligada por um link Intragov com o site Presidente Altino.

Todas as 97 estações mantêm pelo menos um link de dados ativo (contrato Intragov), firewall de borda e switches, mesmo as que já foram concedidas à iniciativa privada.

Além das unidades administrativas e estações ferroviárias, a CPTM possui locais que também dispõem de infraestrutura de TI, sendo compostos por cabines seccionadoras; bases de: manutenção, rede aérea, maquinistas, segurança, monitoramento, Telecom e distribuição elétrica; salas técnicas; subestações elétricas e oficinas, locais estes atendidos por links do contrato Intragov.

Outros locais (unidades administrativas, estações ferroviárias, subestações, base de manutenção e outros) poderão ser criados ou desativados, a critério da CPTM, durante a vigência do contrato.

Outras informações sobre o ambiente atual de TI da CPTM:

- O Hypervisor predominante é Vmware;
- O Sistema Operacional predominante em servidores virtuais é Windows Server;
- O serviço de Correio Eletrônico é Microsoft Exchange;

- DNS, DHCP e IPAM são gerenciados por Infoblox;
- O Proxy é Fortinet;
- Servidores de banco de dados estão em ambiente Oracle Exadata Cloud at Costumer;
- Há também servidores de banco de dados Microsoft SQL Server;
- Os Storages são Dell, NetApp, Fujitsu, Huawei;
- Os Roteadores são Cisco;
- Os Switches são 3Com, ARUBA, Intelbras, Dell, Dlink, PLANET, SMC, TP-link, Cisco, Huawei, HP, Cambium;
- Microsoft e/ou Office 365;
- Os Firewalls são FortiGate;
- O sistema operacional dos Desktops é predominantemente Microsoft Windows;
- Existem servidores e appliances com sistemas operacionais Linux:

  Debian GNU/Linux 10, 11 (64-bit);
  Red Hat Enterprise Linux 7, 8 (64-bit);
  Oracle Linux 8 (64-bit);
  CentOS 8 (64-bit).

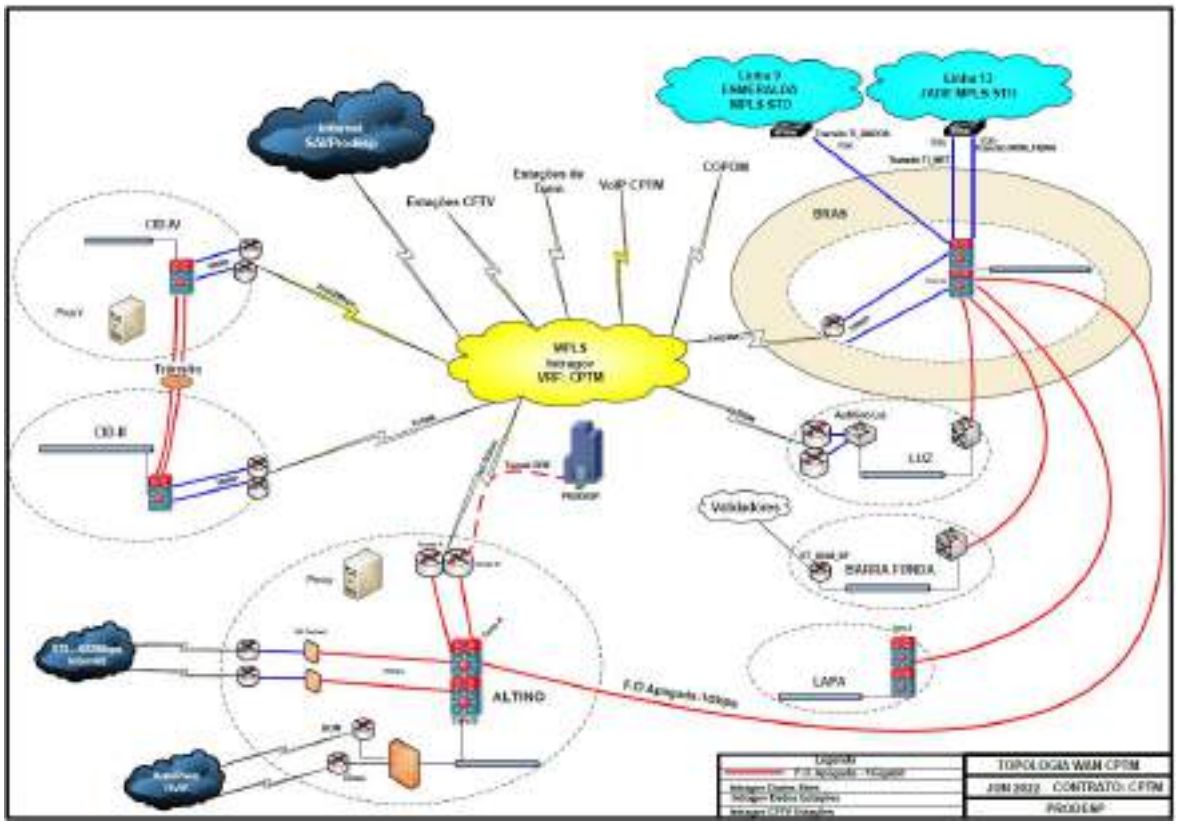
Para efeito de dimensionamento para prestação dos serviços e atendimento aos níveis de serviços, o parque de TI da CPTM está distribuído conforme quadro abaixo de volumes:

Quadro de Volumes

Tipo	Quantidade
Usuários	6000
Desktops	2653
Thin Client	109
Notebooks	398

Servidores físicos	20
Servidores virtuais	193 (229)
Tablets	107
Switches	602
Roteadores	226
Firewalls	6
Links Intragov	212
Racks	315
Storage (TB)	605
Chamados SD	2925/mês

DIAGRAMA ESQUEMÁTICO DA REDE CPTM



2. ESCOPO DOS SERVIÇOS

As atividades objeto desta contratação e que serão executadas pela CONTRATADA englobam as necessidades para o perfeito desempenho das atividades de TI da CPTM, de forma a atender com qualidade, confiabilidade e alta disponibilidade.

Os serviços prestados obrigatoriamente deverão seguir algumas diretrizes metodológicas no sentido de assegurar a qualificação deles, baseadas nas orientações do ITIL 4.

Os recursos necessários à equipe da CONTRATADA (microcomputadores, softwares, links de comunicação para atender soluções estruturadas pela mesma, ferramental elétrico, eletrônico, equipamentos de segurança e mobiliários) para a perfeita execução de suas atividades no ambiente da CPTM. A CONTRATADA deverá estruturar-se da melhor forma que considerar para atender aos acordos de nível de serviço (SLA – Service Level Agreement), respeitando as condições disponíveis de instalação destes, no ambiente de TI da CPTM;

A CONTRATADA fornecerá aos seus empregados, conforme a NR-6 da Portaria 3214/78 do MTE, os EPIs (Equipamentos de Proteção Individual) designados como de sua responsabilidade, bem como treinamento para o seu uso, nos locais onde se faz necessário nas dependências da CPTM;

A CONTRATADA deve dispor de meios que permitam a comunicação imediata com os profissionais alocados e a CPTM, por telefonia celular.

A CONTRATADA deverá disponibilizar ferramentas que permitam à CPTM acompanhar a gestão do objeto deste contrato proporcionando uma gestão efetiva de todos os serviços contratados pela CPTM.

Para o bom desenvolvimento das atividades previstas no escopo desta contratação, é importante que a empresa CONTRATADA venha a atender as seguintes formalidades:

2.1.1. Por solicitação da CPTM ou por iniciativa da CONTRATADA, esta deverá elaborar relatório com as necessidades identificadas no ambiente de TI da CPTM, propondo soluções de atendimento às mesmas, encaminhando-as à CPTM para análise e deliberação;

2.1.2. Por solicitação da CPTM ou por iniciativa da CONTRATADA, realizar estudo técnico específico, com especialistas, que vise identificar necessidade de melhorias no ambiente de TI da CPTM, objetivando as melhores práticas (ex.: procedimentos e/ou soluções para a redução do número de chamados, configuração de equipamentos de TI, performance dos bancos de dados e otimização da segurança, dentre outros conforme objeto do contrato);

2.1.3. O cronograma relativo às adequações no ambiente de TI da CPTM será elaborado pela CONTRATADA e submetido à aprovação da CPTM, caso a caso, de acordo com estratégia da CPTM;

2.1.4. Se as adequações apresentadas fizerem parte da(s) solução(ões) adotadas pela CONTRATADA para atender o objeto desta contratação, compete a esta disponibilizar o necessário para a adequação;

2.1.5. O cronograma de qualquer atividade a ser prestado pela CONTRATADA no objeto desta contratação, no que lhe compete providenciar, realizar, remover, executar, adequar, modificar, apresentar, instalar, não deverá ultrapassar 90 dias corridos para a sua conclusão. A CPTM poderá rever este prazo para maior, em situações específicas, em negociação com a CONTRATADA;

2.1.6. A CONTRATADA deverá instalar, remanejar ou substituir Ativos de TI fornecidos pela CPTM;

2.1.7. A alocação de novos Ativos de TI adquiridos pela CPTM, assim como remanejamento de equipamentos em função da alocação destes novos equipamentos, deverão ser planejados pela CONTRATADA e submetido à CPTM para aprovação antes de sua execução pela CONTRATADA;

2.1.8. Quaisquer intervenções que impactem o ambiente produtivo necessitam de documentação, aprovação e devem ser solicitadas através de processo de Habilitação de Mudança (ITIL4);

2.1.9. Instalar, homologar e configurar os sistemas operacionais e aplicações nas plataformas tecnológicas, de acordo com os procedimentos fornecidos pela CPTM, tanto às aplicações adquiridas como as desenvolvidas internamente ou por fábrica de software;

2.1.10. As senhas masters dos administradores de serviço serão da CPTM, e a CPTM delegará direitos aos administradores da CONTRATADA, os quais deverão utilizar de Certificado Digital através de token para autenticação. Os certificados digitais em token deverão ser especificados e fornecidos pela CONTRATADA;

2.1.11. Realizar a movimentação física de equipamentos de TI nas dependências da CPTM (RMSP), o transporte de equipamentos entre unidades da CPTM será executado exclusivamente por empresa ou equipe técnica especializada e devidamente habilitada para essa finalidade, não sendo essa atividade de responsabilidade da CONTRATADA.

2.1.12. A movimentação interna de equipamentos, restrita ao deslocamento dentro da mesma unidade, será pela CONTRATADA apenas para equipamentos de pequeno porte, tais como: switches de borda, access points, servidores de pequeno porte, notebooks, desktops, monitores, impressoras de pequeno porte, scanners, telefones IP e periféricos em geral.

2.1.13. Equipamentos de maior porte, como racks, switches de núcleo, enclosures, storages, unidades de backup, no-breaks, grupos geradores, salas cofre, entre outros, somente poderão ser movimentados em conformidade com as especificações técnicas dos respectivos fabricantes, por equipes formalmente habilitadas por estes e fornecidos pela CONTRATANTE, utilizando equipamentos e ferramentais adequados, mediante planejamento prévio e controle da operação.

2.1.14. As CONTRATADAS — tanto a responsável pela movimentação quanto a responsável pelo transporte — não poderão ser responsabilizadas por eventuais avarias nos equipamentos, bem como por furto ou roubo do veículo durante o transporte, desde que

comprovada a inexistência de culpa ou negligência por parte delas. A apuração de eventual responsabilidade se dará mediante conclusão de sindicância administrativa conduzida pela CONTRATANTE e/ou investigação formalmente conduzida pelos órgãos de segurança pública, devendo ser acompanhada do respectivo boletim de ocorrência que registre os fatos e fundamente a apuração realizada.

O presente Termo de Referência visa contratar soluções e serviços especializados na área de TI com o seguinte escopo:

2.1.15. Solução de gestão do ambiente de TI

2.1.16. Serviço de coordenação de Operação de TI e Projetos;

2.1.17. Serviço de monitoramento de ambiente de TI (NOC);

2.1.18. Serviço de gestão e operação do ambiente de rede corporativa;

2.1.19. Serviço de administração e operação dos ambientes de banco de dados;

2.1.20. Serviço de gestão e operação do ambiente virtualizado;

2.1.21. Serviço de gestão e operação de soluções de armazenamento;

2.1.22. Serviço de gestão e operação da solução de Backup;

2.1.23. Serviço de segurança cibernética, tratamento e resposta à incidentes;

2.1.24. Solução de Firewall;

2.1.25. Solução estendida de detecção e resposta, segurança de endpoints e rede;

2.1.26. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados e informações contidos em documentos e em mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CPTM a tais documentos;

2.1.27. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou

de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da CPTM;

2.1.28. A CONTRATADA deverá assegurar o sigilo das informações, documentos e bancos de dados da CPTM, e adotar todas as providências necessárias para garantir sigilo de toda e qualquer informação a que ver acesso em função da prestação dos serviços previstos neste TR, respondendo administrativa, civil e penalmente por qualquer violação desse preceito;

2.1.29. A CONTRATADA deverá colaborar com procedimentos de investigação ou auditoria, em especial os em face do uso indevido das informações disponibilizadas para a execução das atividades;

2.1.30. Todo o material, documentos, softwares, códigos, tecnologias, know-how e demais propriedades intelectuais fornecidas pela CPTM ou desenvolvidos durante a execução dos serviços de TI são de exclusiva propriedade desta última;

2.1.31. Em caso de qualquer violação de sigilo ou uso indevido da propriedade intelectual da CPTM por parte dos profissionais alocados da

2.1.32. CONTRATADA, esta será inteiramente responsável pelas consequências legais, administrativas e financeiras decorrentes de tais ações;

2.1.33. A CPTM reserva-se o direito de, a qualquer momento, solicitar à CONTRATADA a substituição de qualquer profissional alocado que esteja envolvido em violação de propriedade intelectual ou outras condutas inadequadas relacionadas aos serviços prestados;

2.1.34. A responsabilidade da CONTRATADA em relação à proteção de propriedade intelectual sobreviverá à rescisão ou término deste contrato, permanecendo válidas e vinculantes as obrigações de sigilo e confidencialidade durante o período de vigência contratual e mesmo após o seu encerramento.

3. SOLUÇÃO DE GESTÃO DO AMBIENTE DE TI

O aplicativo a ser utilizado para a Gestão do ambiente de TI deverá atender no mínimo as funcionalidades a seguir:

3.1.1. Efetuar o gerenciamento do ambiente de TI correlacionando eventos das plataformas que compõe o Framework de Gerenciamento da CONTRATADA;

3.1.2. Possuir uma arquitetura multicamada focada em eficiência e escalabilidade;

3.1.3. Descobrir de forma automática equipamentos de TI, sistemas operacionais e recursos, topologia de rede com seus periféricos (firewall (UTM), switches) e seus relacionamentos, permitindo à organização mapear de maneira fácil e precisa todo o ambiente de TI;

3.1.4. Coletar automaticamente as informações de diferentes elementos do ambiente de TI e identificar mudanças de estado e eventos pelos ativos quando forem ligados ou reinicializados, em um repositório de objetos (base de dados);

3.1.5. Oferecer dashboards interativos e amigáveis que permitam à CPTM uma visualização dos eventos críticos de todo ambiente, com drill down;

3.1.6. Permitir que de uma simples interface, a CPTM possa gerenciar a disponibilidade de suas LAN, SAN e WAN;

3.1.7. Possuir capacidade de consoles distribuídas de gerenciamento, baseadas na plataforma operacional Windows Server, além da visão geral, criando visões segmentadas dos componentes de gerenciamento especificados;

3.1.8. Dispor de tecnologia de agentes que permita à CPTM monitorar seus dispositivos, sistemas, aplicações e os bancos de dados corporativos (Oracle, MS SQL Server e Postgre), através da detecção, filtragem e envio de eventos significantes, permitindo que

os administradores e/ou Gestor de TI, facilmente entendam as mudanças e identifiquem problemas de desempenho;

3.1.9. Dispor de capacidade de gerenciamento proativo na prevenção de problemas e recursos que permita retroagir no tempo (histórico de eventos) e assim permitir à CPTM não somente identificar a sequência de eventos que originou problemas ou gargalos, como também evitar novas ocorrências;

3.1.10. Prover alarmes gerando notificação aos administradores e/ou Gestor de TI;

3.1.11. Permitir aos administradores e/ou Gestor de TI, através de visões parametrizadas, receber um conjunto de eventos, para atender necessidades da gestão;

3.1.12. Permitir que os administradores e/ou Gestor de TI possam receber notificações de eventos por e-mail. A CPTM definirá quais eventos devem gerar notificações;

3.1.13. Possuir recursos para que as ações dos administradores via ferramenta de gerenciamento sejam passíveis de auditoria contendo informações de, pelo menos, data/hora, nome / identificação do administrador e local de onde foi realizada a operação;

3.1.14. Prover criação de mapas de visualização que permitam à CPTM observar seu ambiente de TI;

3.1.15. Ter a capacidade de acesso por múltiplos usuários;

3.1.16. Possuir tratamento de alertas em tempo real permitindo programação e execução de ações de notificação;

3.1.17. Possuir gerenciamento corporativo e centralizado de todo o ambiente de TI;

3.1.18. Possuir console gráfica que centralize todas as ocorrências gerenciadas que estejam acontecendo na rede ou em um segmento desta;

3.1.19. Notificar quando tarefas não iniciam ou terminam dentro dos horários especificados;

3.1.20. Permitir gerenciamento em tempo real de métricas de todo o ambiente de TI, possibilitando a criação de limites (thresholds) configuráveis online;

3.1.21. Identificar componentes que estejam: consumindo recursos excessivos, falhas de recursos operacionais, atuando preventivamente;

3.1.22. Proporcionar rápida solução de problemas, contando com um gerenciamento simplificado de políticas, diagnóstico automático de problemas e autocorreção quando possível;

3.1.23. Para os sistemas operacionais Windows Server, os agentes devem acompanhar, em tempo real, as seguintes métricas básicas:

3.1.24. Monitoração de processos do sistema operacional e reinicialização automática de processos críticos;

3.1.25. Utilização, crescimento e estado de pools de file systems específicos;

3.1.26. Crescimento e alterações em arquivos;

3.1.27. Estado dos processos e número de threads e instances de processos ativos;

3.1.28. Estados dos serviços do sistema;

3.1.29. Percentagem de memória que está sendo utilizada (percentagem de memória física e a percentagem de espaço de swap disponível);

3.1.30. Utilização de cada processador de um mesmo servidor;

3.1.31. Alterações no registry do sistema;

4. SERVIÇO DE COORDENAÇÃO DE OPERAÇÃO DE TI E PROJETOS

A CONTRATADA deverá:

4.1.1. Apoiar na definição de Estratégias, Políticas e Padrões da Área de TI;

4.1.2. Alcançar melhoria e excelência na prestação dos serviços oferecidos através de processos baseados nas melhores práticas descritas pelo ITIL 4 e COBIT;

4.1.3. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

4.1.4. Melhorar a prestação da qualidade dos serviços através do aumento do nível de maturidade dos processos;

4.1.5. Promover sugestões à CPTM visando a melhoria de uso das ferramentas, processos, gestão e alocação de recursos;

4.1.6. Promover a visão de Gerenciamento de Serviços para todos os níveis;

4.1.7. Elaborar e implantar atividades de melhoria contínua dos processos;

4.1.8. Elaborar e recomendar melhorias nos fluxos de trabalho dos profissionais da CONTRATADA e da CPTM;

4.1.9. Elaborar relatórios de riscos do ambiente tecnológico da CPTM.

4.1.10. Propor planos de continuidade de serviços de TI e submetê-los à aprovação da CPTM;

4.1.11. Alertar o gestor do contrato, de forma proativa, sobre qualquer problema, anormalidade, falta de recursos ou comportamento não previsto que possam causar impactos nos serviços de TI;

4.1.12. Realizar gestão e auditoria dos planos de continuidade de serviços de TI;

4.1.13. Elaborar relatórios de entrega de serviços e medições contratuais;

4.1.14. Realizar análise e diagnóstico de dados, utilizando ferramentas de Business Intelligence (BI) para suportar tomadas de decisão;

4.1.15. Colaborar com informações, sugestões e experiências, a fim de contribuir para o desenvolvimento contínuo da operação e melhoria de processos;

4.1.16. Realizar elaboração, padronização e manutenção de procedimentos, modelos e documentos de apoio aos processos;

4.1.17. Identificar oportunidades de melhoria, evoluções e correções nos processos, promovendo inovação e alinhamento estratégico;

4.1.18. Planejar e conduzir análises estruturadas de problemas, aplicando metodologias como PDCA, 5W2H ou Diagrama de Ishikawa;

4.1.19. Realizar treinamentos sobre processos operacionais e boas práticas de mercado, sempre que necessário;

4.1.20. Garantir a aderência dos processos às normas e padrões corporativos, como ITIL 4, COBIT e frameworks de governança, quando aplicável;

4.1.21. Apoiar auditorias internas e externas relacionadas aos processos organizacionais.

4.1.22. Apoiar os gestores nas melhores práticas sugerindo melhorias nos processos;

4.1.23. Realizar criação e análise de indicadores de desempenho de processos;

4.1.24. Identificar e otimizar processos críticos;

4.1.25. Interagir com equipes e gestores da operação;

4.1.26. Participar da elaboração, documentação e implementação de processos;

4.1.27. O serviço deverá estar disponível em horário comercial, das 9h às 18h, de segunda a sexta-feira, e contar também com Suporte Emergencial em regime de sobreaviso 24x7x365, no qual um profissional da equipe permanecerá disponível fora do expediente para atendimentos quando acionado.

5. SERVIÇO DE MONITORAMENTO DE AMBIENTE DE TI (NOC)

As seguintes condutas são esperadas:

5.1.1. A CONTRATADA deverá prover serviço de monitoramento da infraestrutura de TI em NOC (Network Operations Center / Centro de Operações de Rede), visando o monitoramento e disponibilidade da infraestrutura de TI da CPTM, incluindo seus ativos, itens de configuração e os serviços associados;

5.1.2. O monitoramento dos serviços de TI deve ser completo e suficiente para ser efetivo quanto à detecção preventiva de incidentes, antes que venham a causar indisponibilidades;

5.1.3. O monitoramento deverá ser apoiado por ferramentas de monitoramento e diagnóstico específicas para tal, as quais são de responsabilidade da CONTRATADA;

5.1.4. Quando, no monitoramento, for caracterizado o evento de incidente, este deve ser registrado de forma automática na Solução de Gerenciamento de Serviços de TI, devendo o operador do serviço de monitoramento ser capaz de atuar tecnicamente para restabelecer o serviço ou o ativo de TI nos casos em que o acesso administrativo/especializado ao recurso não se fizer necessário, com base em parâmetros e scripts pré-definidos;

5.1.5. A CONTRATADA deverá, por meio de recursos da sua equipe, realizar rotineiramente o mapeamento das oportunidades de melhoria do monitoramento dos ativos e serviços de TI mantidos pelo CPTM;

5.1.6. A partir desse mapeamento, a CONTRATADA deverá implementar ferramentas de monitoramento de ativos e serviços com a automação das ações conforme uma matriz de tomada de decisão.

5.1.7. A CONTRATADA deverá ainda, propor e implementar, caso autorizada, rotinas automatizadas para testes de ativos, serviços e sistemas, tanto para medição da disponibilidade e desempenho, quanto para testes pós mudanças no ambiente.

5.1.8. Durante o período de implantação (transição operacional) do contrato, deverá ser elaborado um plano de ação para este ciclo de automação de monitoramento de ativos e serviços.

5.1.9. A CONTRATADA deverá acompanhar fornecedores quando necessário;

5.1.10. Prover o serviço em regime de 24 X 7 X 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

6. SERVIÇO DE GESTÃO E OPERAÇÃO DO AMBIENTE DE REDE CORPORATIVA

A CONTRATADA deverá:

6.1.1. Executar as atividades relacionadas à administração, operação, implantação e suporte aos Ativos de Rede e Comunicação, que sustentam a comunicação de dados, voz, vídeo, videoconferência, LAN e Wireless;

6.1.2. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

6.1.3. Propor e executar melhorias no ambiente;

6.1.4. Orientar as equipes de suporte quanto aos dispositivos e ambientes Lan;

6.1.5. Acompanhar a equipe de infraestrutura nos serviços de manutenção ligados a sistema estruturado de lógica e telefonia predial convencional ou IP;

6.1.6. Executar e apoiar as adequações de instalação ou remanejamento de elementos ativos de rede e backbones;

6.1.7. Executar e apoiar as adequações de instalação ou remanejamentos de “Access Points” de rede sem fio;

6.1.8. Executar instalação física e remanejamento de servidores/racks, garantindo as funcionalidades da rede em todas as localidades em que a CPTM atua;

6.1.9. Prover as adequações de instalação e os remanejamentos de cabeamento estruturado, assegurando as funcionalidades lógicas no Data Center, com materiais fornecidos pela CONTRATANTE, ficando excluída, entretanto, a execução de atividades de certificação de cabos e fusão de fibra óptica;

6.1.10. Prover as adequações de instalação ou os remanejamentos do sistema estruturado do backbone e do Data Center, garantindo as funcionalidades lógicas por meio de fibra óptica, com materiais fornecidos pela CONTRATANTE, ficando excluída, entretanto, a execução de atividades de certificação de cabos e fusão de fibra óptica;

6.1.11. O serviço deverá estar disponível em horário comercial, das 7h às 19h, de segunda a sexta-feira, e contar também com Suporte Emergencial em regime de sobreaviso 24x7x365, no qual um profissional da equipe permanecerá disponível fora do expediente para atendimentos quando acionado.

7. SERVIÇO DE ADMINISTRAÇÃO E OPERAÇÃO DOS AMBIENTES DE BANCO DE DADOS

A CONTRATADA deverá:

7.1.1. Elaborar, implantar, documentar e manter normas de administração de dados e de gerenciamento de banco de dados;

7.1.2. Administrar, instalar, customizar e manter os SGBD's (Sistemas de Gerenciamento de Banco de Dados) dos sistemas corporativos;

7.1.3. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

7.1.4. Desenvolver e manter procedimentos de consulta, captação, atualização e armazenamento de dados;

7.1.5. Monitorar e analisar o desempenho de acesso às bases de dados;

7.1.6. Definir e executar rotinas de alimentação e extração de dados;

7.1.7. Realizar integração das atividades com a área de desenvolvimento e manutenção de sistemas;

7.1.8. Suporte, administração e operação em banco de dados Oracle e MS SQL Server (DBA);

7.1.9. Atualizar banco de dados (produção, desenvolvimento, homologação, redundante) através da Gestão de Mudanças, com relação à patchs, novos releases e versões;

7.1.10. Monitorar do banco de dados, clusters e servidores;

7.1.11. Documentar os bancos de dados (processos, roteiros, produtos e arquitetura);

7.1.12. Elaborar relatórios consolidado dos bancos de dados (capacidade, desempenho, eventos);

7.1.13. Gerenciar e administrar permissão de acesso aos bancos de dados;

7.1.14. Analisar a implementação de serviços (análise do impacto de novos projetos da CPTM);

7.1.15. Implementar serviços (se aprovado na análise);

7.1.16. Implementar novos projetos;

7.1.17. Prover manutenção corretiva dos bancos de dados com recuperação de backup (serviços, instâncias, estrutura de dados, sistemas operacionais);

7.1.18. Configurar serviço em servidor de banco de dados;

7.1.19. Implementar projetos de banco de dados (desenvolvimento, validação e produção);

7.1.20. Migrar banco de dados para novas versões disponibilizadas pelo fabricante ou para outros equipamentos;

7.1.21. . Realizar a manutenção de stored procedures, funções e programas de rotinas, utilizando ferramentas do SGBD ou de mercado, sendo certo que a elaboração e o desenvolvimento desses artefatos são de responsabilidade das equipes de análise de dados e

de desenvolvimento da CONTRATANTE ou de suas demais contratadas;

7.1.22. Elaborar, revisar, verificar, preparar e implementar e customizar produtos do SGBD, incluindo migrações de versões, planejamento e execução de rotinas de testes (roteiros, programas) implementação de padrões de interface e gerenciamento de bases de dados dos SGBD;

7.1.23. Elaborar a definição de padrões de interface: a administração de base de dados, ferramentas de monitoração de banco de dados, instalação e customização de banco de dados, produtos e ferramentas que compõem o ambiente SGBD da CPTM;

7.1.24. Prover suporte no uso de ferramentas ou ambientes específicos, atividades que requeiram conhecimentos de negócio;

7.1.25. Subsidiar a elaboração dos relatórios de entrega de serviço e medição contratual.

7.1.26. Utilizar no gerenciamento e administração dos bancos de dados da CPTM, profissionais qualificados e certificados pelos fornecedores do fabricante do banco de dados. Os SGBD em uso na CPTM são: Oracle e MS SQL Server;

7.1.27. Efetuar um levantamento de todo ambiente computacional que será suportado, contemplando as seguintes atividades:

7.1.27.1. Levantamento de servidores de dados, com a identificação da tecnologia e sistema operacional, produtos e versões de banco de dados;

7.1.27.2. Distribuição dos servidores no site principal, sites secundários e sites de contingência;

7.1.27.3. Mapa do ambiente e soluções de contingência;

7.1.27.4. Levantar a situação atual de todo ambiente de banco de dados, diagnosticar os eventuais problemas existentes;

7.1.27.5. Identificar e indicar, se for o caso, a necessidade de execução de tunning do ambiente de banco de dados, visando a melhoria de desempenho;

7.1.27.6. Identificar e indicar, se for o caso, eventuais atividades que a CONTRATADA terá que realizar, extra ambiente de banco de dados (sistema operacional, ambiente de BI, redes, storage) que resultará em melhoria de desempenho, segurança, exceto em necessidade de hardware, o qual será providenciado pela CPTM;

7.1.27.7. Documentar e manter atualizada a documentação do ambiente de banco de dados;

7.1.27.8. Apontar e executar as atividades iniciais diagnosticadas para a melhoria do ambiente;

7.1.27.9. Realizar o levantamento acima citado, para a plena absorção de conhecimento do ambiente computacional de banco de dados, em até 90 dias corridos após a emissão da Ordem de Serviço;

7.1.28. Analisar e implementar ações de hardening;

7.1.29. Manter base de conhecimento de procedimentos técnicos atualizada.

7.1.30. Acompanhar fornecedores quando necessário;

CONTRATADA deverá:

7.1.31. Atuar na manutenção preventiva dos Sistemas Gerenciadores de Banco de Dados - SGBD (serviços, instâncias, estrutura de dados, sistema operacionais, Storage e rede);

7.1.32. Atuar no uso de ferramentas ou ambientes específicos, atividades que requeiram conhecimentos de negócio;

7.1.33. Dimensionar carga e reservas de RAM, PGA e SGA;

7.1.34. Aplicar melhores práticas de acomodação de instâncias e datafiles;

7.1.35. Definir a arquitetura do ambiente como um todo, elaborando o planejamento de capacidade;

7.1.36. Esclarecer dúvidas, configurações, prover e realizar a solução de problemas básicos, críticos e emergenciais em toda plataforma dos SGBD da CPTM;

7.1.37. Realizar atividades corretivas e preventivas, previamente programadas de acordo com SLA's definidos;

7.1.38. Propor definição de padrões de interface, à administração da base de dados, instalação e customização de banco de dados, gateways, ferramentas de monitoração de banco de dados e ferramentas que compõe o ambiente dos SGBD em uso na CPTM;

7.1.39. Estruturar e revisar a definição de arquitetura do ambiente como um todo e no planejamento de capacidade, integração da gerência de vários projetos através da visão corporativa do Sistema de Informação e Healthcheck (Controle de Qualidade), do ambiente dos SGBD em uso na CPTM;

7.1.40. Planejar todas as atividades a serem desenvolvidas, apresentando-as para deliberação em reunião de GMUD, do ambiente dos SGBD em uso na CPTM;

7.1.41. Submeter as customizações oriundas de análise de tunning, a apreciação da CPTM antes de sua efetivação;

7.1.42. Alocar profissionais cuja formação e experiência atendam aos perfis especificados neste instrumento, do ambiente dos SGBD em uso na CPTM;

7.1.43. Realizar atividades corretivas e preventivas, previamente programadas de acordo com SLA's definidos, do ambiente dos SGBD em uso na CPTM;

7.1.44. O serviço deverá estar disponível em horário comercial, das 7h às 19h, de segunda a sexta-feira, e contar também com Suporte Emergencial em regime de sobreaviso 24x7x365, no qual um profissional da equipe permanecerá disponível fora do expediente para atendimentos quando acionado.

7.1.45. Agir na ocorrência de chamado (incidente), e de acordo com sua classificação de prioridade, provendo sua solução dentro da SLA definido;

7.1.46. Gerar relatórios das atividades a serem executadas pela CONTRATADA, referentes ao ambiente dos SGBD em uso na CPTM;

8. SERVIÇO DE GESTÃO E OPERAÇÃO DO AMBIENTE VIRTUALIZADO

A CONTRATADA deverá:

8.1.1. Instalar, atualizar, configurar, customizar e suportar todos os servidores físicos e virtuais, sistemas operacionais e sistemas de virtualização que compõe a infraestrutura do datacenter do CPTM;

8.1.2. Criar procedimentos de correção de falhas que serão adotados pela equipe do Monitoramento (NOC);

8.1.3. Diagnosticar e resolver problemas de desempenho nos ambientes suportados;

8.1.4. Verificar periodicamente os logs dos servidores, sistemas de storages e virtualização de modo a agir proativamente em casos de problemas ou comportamentos não esperados;

8.1.5. Abrir e acompanhar chamados técnicos dos fabricantes das soluções instaladas;

8.1.6. Implementar e Administrar serviços cluster e webserver (IIS, Apache);

8.1.7. Realizar mudanças de configuração, novas configurações, novas implantações e todas as atividades necessárias, nos ambientes suportados, de modo a atender plenamente os serviços de TI da CPTM;

8.1.8. Projetar, implantar e validar procedimentos de alta disponibilidade;

8.1.9. Acompanhar o uso de recursos físicos pelo ambiente de virtualização, agindo proativamente, antes do esgotamento de recursos físicos dele;

8.1.10. Efetuar instalação e atualização de aplicações nos ambientes mantidos pela CPTM, incluindo a atualização, deploy de aplicações e instalação ou configuração de componentes, seguindo procedimentos elaborados pelos serviços de administração e suporte aos servidores de aplicação, e aprovados pelo processo de habilitação de mudança da CPTM;

8.1.11. Realizar a criação de políticas de grupos de operação, de backup, de alertas, de gerenciamento de espaço, de governança de dados dos produtos Microsoft adquiridos pela CPTM;

8.1.12. Configurar permissões de usuários e/ou grupo dos produtos Office/Microsoft 365;

8.1.13. Realizar a abertura e acompanhar chamados para suporte do fabricante sobre as ferramentas do Office/Microsoft 365 e suporte Unified da Microsoft.

8.1.14. Atender a solicitações de arquiteturas, permissões de acesso do Office/Microsoft 365;

8.1.15. Manter controle e padronização das configurações dos servidores de aplicação em uso na CPTM;

8.1.16. Verificar, diariamente, se as tarefas estão sendo executadas de acordo com os níveis de serviço contratados;

8.1.17. Analisar o ambiente utilizando métricas de desempenho, assegurando a continuidade, escalabilidade e desempenho adequado;

8.1.18. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

8.1.19. Executar tarefas administrativas gerais, incluindo, mas não se limitando, a criação e gerenciamento de usuários, permissões de acesso, manutenção de logs, auditorias e configuração do firewall do Windows para bloqueios;

8.1.20. Administrar File Servers Microsoft, utilizando recursos como ACL's, ABE, Shadow Copy e cotas de disco;

8.1.21. Gerenciar e configurar Microsoft AD DC (incluindo instalação, configuração de GPOs, gerenciamento de replicações inter-sites, relação de confiança entre domínios, e criação de AD RODC);

8.1.22. Aplicar atualizações de segurança recomendadas para sistemas operacionais, mantendo a estabilidade e o funcionamento ideal;

8.1.23. Garantir backups regulares e restauráveis para proteção de dados em caso de falhas;

8.1.24. Responder a incidentes e alertas, implementando soluções de contorno e propondo soluções definitivas;

8.1.25. Configurar a coleta de dados de performance com Perfmon para indicadores críticos;

8.1.26. Realizar o planejamento de capacidade para ambientes de servidores Windows, otimizando recursos;

8.1.27. Desenvolver scripts em Batch, VBS e PowerShell para automação de processos administrativos;

8.1.28. Elaborar e manter documentações técnicas detalhadas sobre servidores, serviços e infraestrutura, incluindo topologias e configurações;

8.1.29. Implementar serviços Microsoft NLB para balanceamento de carga;

8.1.30. Instalar, configurar e desativar servidores e softwares relacionados;

8.1.31. Configurar e manter serviços essenciais tais como: DHCP, DNS, IIS, WSUS, Print Server, Microsoft Failover Clustering e AD CS;

8.1.32. Projetar, implementar e manter ambientes híbridos, integrando soluções *on-premises* com nuvens públicas;

8.1.33. Auxiliar nos testes de backup e restore, e efetuar o restore de todos os serviços inerentes à rede e Windows Server;

8.1.34. Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com serviços de operação do ambiente de Virtualização;

8.1.35. Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com os sistemas operacionais Microsoft;

8.1.36. Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com sistemas operacionais baseados em Linux;

8.1.37. Executar mudanças, migrações, atualizações, implantações e testes de novos produtos na plataforma Linux.

8.1.38. Executar serviços nos servidores Linux, tais como gerenciamento de discos, parametrização dos sistemas, atualização de versões dos sistemas operacionais e aplicativos, aplicação de correções e patches.

8.1.39. Gerenciar e manter a administração dos serviços de DNS, DHCP e Gerenciamento de IPs através da ferramenta INFOBLOX, mantida pela CPTM;

8.1.40. Analisar e implementar ações de *hardening*;

8.1.41. Manter base de conhecimento de procedimentos técnicos atualizados;

8.1.42. Acompanhar fornecedores quando necessário;

8.1.43. A CPTM utiliza solução da VMware para a virtualização de seu parque computacional. A CONTRATADA deverá operar, gerenciar e proceder com as atividades:

8.1.43.1. Dimensionar hardware;

8.1.43.2. Monitorar e administrar os componentes e elementos de virtualização;

8.1.43.3. Administrar servidores de virtualização;

8.1.43.4. Criar, remover e editar máquinas virtuais e OS suportados;

8.1.43.5. Converter servidores físicos em virtuais;

8.1.43.6. Gerenciar o controle de acesso de usuários;

8.1.43.7. Gerenciar o ambiente virtualizado com a solução VMware;

8.1.43.8. Gerenciar e monitorar alarmes;

8.1.43.9. Gerenciar e monitorar indicadores e marcadores de carga e recursos;

8.1.43.10. Gerenciar snapshots e backup´s;

8.1.43.11. Restaurar backup's;

8.1.43.12. Distribuir e alocar dos recursos em pools de CPU, memória e I/O;

8.1.43.13. DRS Cluster (Distributed Resource Scheduler);

8.1.43.14. Migrações automáticas de máquinas virtuais entre os hosts;

8.1.43.15. Criar HA Clusters;

8.1.43.16. Operar Linha de Comando via SSH (CLI) o Hypervisor.

8.1.43.17. Atualização de firmware realizada para equipamentos com serviços de suporte e manutenção ativos – adquiridos pela CONTRATANTE, prestados pelos fabricantes ou seus representantes autorizados;

8.1.43.18. Em casos de ausência de serviços de suporte e manutenção de equipamentos, sendo necessária atualização de firmware destes, a CONTRATADA deverá apresentar relatório de riscos desta execução, solicitando a aprovação da

CONTRATANTE para execução e anuência quanto aos riscos apontados - sem responsabilidade ou ônus à CONTRATADA em caso de falhas ocorridos após a realização desta atividade;

8.1.43.19. Implantar (deploy) e dar suporte aos servidores (hosts) para a plataforma VMware;

8.1.43.20. Realizar a conversão de máquinas físicas ou virtuais de outras plataformas para dentro do ambiente VMware VCenter e vice-versa;

8.1.43.21. Realizar a instalação e configuração dos recursos, clusters, eventos e *features* do servidor vCenter primário e secundário;

8.1.43.22. Realizar criação, manutenção e suporte das imagens (templates VMware) de sistemas operacionais;

8.1.43.23. Configurar e gerenciar a capacidade dos componentes da infraestrutura VMware, incluindo hosts, máquinas virtuais, data storages e switches virtuais distribuídos;

8.1.43.24. Realizar a configuração e monitoração para garantir a escalabilidade e performance do ambiente através das funções: VMware vMotion, Storage Motion, High Availability, Patch Management com o vCenter Update Manager, Data Protection e VMware Data Recovery;

8.1.43.25. Realizar integração e sincronização de plataformas heterogêneas (Windows e Linux);

8.1.43.26. Apoiar os profissionais de suporte nas manutenções de equipamentos nos Data Centers, sendo responsabilidade da CONTRATANTE prover o suporte e a manutenção relacionados ao hardware e ao software VMware;;

8.1.43.27. Elaborar planilhas, controles e relatórios para a equipe, bem como documentar procedimentos;

8.1.43.28. Realizar a configuração de clusters;

9. SERVIÇO DE GESTÃO E OPERAÇÃO DE SOLUÇÕES DE ARMAZENAMENTO;

A CONTRATADA deverá:

9.1.1. Realizar a manutenção, gerenciamento e administração de equipamentos em redes SANs (storage area networks);

9.1.2. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

9.1.3. Otimizar e realizar configuração de multipathing de I/O;

9.1.4. Configurar soluções de armazenamento (storages);

9.1.5. Gerenciar soluções de armazenamento SAN e NAS (iSCSI.NFS);

9.1.6. Realizar atualização de versão de software das soluções de armazenamento;

9.1.7. Em casos de ausência de serviços de suporte e manutenção de equipamentos, sendo necessária atualização de software destes, a CONTRATADA deverá apresentar relatório de riscos desta execução, solicitando a aprovação da CONTRATANTE para execução e anuência quanto aos riscos apontados - sem responsabilidade ou ônus à CONTRATADA em caso de falhas ocorridos após a realização desta atividade;

9.1.8. Realizar análise de relatórios das soluções de armazenamento;

9.1.9. Realizar análise e verificação de capacidade para LUN, Volumes e Aggregate;

9.1.10. Monitorar e executar análise de performance, capacidade e consumo dos recursos de hardware das soluções de armazenamento;

9.1.11. Realizar análise de logs das soluções de armazenamento e realizar o gerenciamento do crescimento de informações;

9.1.12. Criar, configurar, excluir e documentar Zoning, Alias, NFS, LUN, Volumes, RAID, Storage Groups e Storage Pools;

9.1.13. Criar e configurar sistemas de arquivos;

9.1.14. Criar, excluir, alterar snapshots;

9.1.15. Proceder com a configuração de NFS/CIFS, criação ou configuração de cotas de armazenamento;

9.1.16. Configurar Qtree em NAS;

9.1.17. Checar atualizações de firmware e instalar se necessário;

9.1.18. Em casos de ausência de serviços de suporte e manutenção de equipamentos, sendo necessária atualização de firmware destes, a CONTRATADA deverá apresentar relatório de riscos desta execução, solicitando a aprovação da CONTRATANTE para execução e anuência quanto aos riscos apontados - sem responsabilidade ou ônus à CONTRATADA em caso de falhas ocorridos após a realização desta atividade;

9.1.19. Checar e gerenciar o espaço disponível nas soluções de armazenamento (on premises ou nuvem);

9.1.20. Verificar saúde das soluções de armazenamento;

9.1.21. Realizar documentação do ambiente de armazenamento em geral;

9.1.22. Analisar e implementar ações de hardening;

9.1.23. Analisar e implementar soluções para melhoria de desempenho (Tuning), escalonamento de demandas, balanceamento de carga e alta disponibilidade;

9.1.24. Aplicar as melhores práticas de configuração e segurança no ambiente de armazenamento e SAN;

9.1.25. Manter base de conhecimento de procedimentos técnicos atualizada.

9.1.26. Acompanhar fornecedores quando necessário;

10. SERVIÇO DE GESTÃO E OPERAÇÃO DA SOLUÇÃO DE BACKUP;

A CONTRATADA deverá**:**

10.1.1. Executar, manter, atualizar, implantar e apoiar na criação dos planos de backup da CPTM;

10.1.2. Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;

10.1.3. Seguir ao estabelecido na Política de Backup vigente existente;

10.1.4. Realizar a configuração de jobs, configuração de políticas para backup/restore, recuperação de base de dados existentes no ambiente CPTM, atualizar os pacotes de correção, checar relatório do backup, checar rotina de backup, configuração de desduplicação;

10.1.5. Realizar testes de restore com definição de frequência a critério da CPTM (Política de Backup vigente);

10.1.6. Analisar Logs das soluções de backup em uso pela CPTM,

10.1.7. Elaborar relatórios técnicos, análise de logs das rotinas de backup e restore, movimentar cópias entre datacenters, alterar retenção dos backups, instalar/desinstalar agente de backup, realizar/modificar/excluir backup, restaurar cópias de segurança;

10.1.8. Aplicar as melhores práticas de configuração, segurança, alta disponibilidade, desempenho (tuning) dos serviços de backup;

10.1.9. Criar/alterar/remover rotinas de backup;

10.1.10. Executar backup;

10.1.11. Implantar estrutura de Backup;

10.1.12. Realizar limpeza de logs obsoletos conforme a Política de Backup vigente;

10.1.13. Realizar recuperação dos dados cobertos pelos planos de backup;

10.1.14. Acompanhar fornecedores quando necessário;

10.1.15. Elaborar e atualizar a documentação da solução de backup;

10.1.16. Manter base de conhecimento de procedimentos técnicos atualizada.

11. SERVIÇO DE SEGURANÇA COM TRATAMENTO E RESPOSTA À INCIDENTES CIBERNÉTICOS

A CONTRATADA deverá:

11.1.1. Suportar as outras equipes e usuários em assuntos relacionados à Segurança da Informação.

11.1.2. Realizar atividades relacionadas à administração, operação, implantação e suporte de equipamentos e soluções de segurança.

11.1.3. Realizar análises de risco e construção de documentos de Análise de Impacto aos Negócios (BIA), com base nas vulnerabilidades do ambiente de TIC.

11.1.4. Propor, e quando da responsabilidade da equipe de segurança, executar melhorias no ambiente aprovadas pela CPTM.

11.1.5. Conduzir análises nos aplicativos e componentes de infraestrutura para avaliar a confidencialidade, integridade, disponibilidade, autenticidade e confiabilidade dos serviços.

11.1.6. Conduzir a identificação dos riscos dos ativos e impactos aos negócios.

11.1.7. Conscientizar, educar e realizar treinamentos em segurança da informação de acordo com a estratégia de comunicação.

11.1.8. Avaliar a segurança física e lógica dos ambientes de TI, realizar gerenciamento de mídias removíveis tais como pendrivers, HD Externos, leitores de CDs e DVDs e dispositivos móveis, dois pentestes anuais.

11.1.9. Realizar acompanhamento e monitoração das atividades executadas pela equipe de segurança ou por outras equipes de TI, em atividades relacionadas à Segurança da Informação.

11.1.10. Coletar evidências de incidentes de segurança da informação para elaborar relatórios de aprendizado.

11.1.11. Garantir a conformidade com requisitos legais, propriedade intelectual, proteção dos registros organizacionais, privacidade de informações pessoais.

11.1.12. Deverá atuar, em caso de incidentes de segurança da informação e cibernéticos, suportando a CPTM na preparação de

planos de resposta, detecção e análise, contenção, erradicação e recuperação do incidente.

11.1.13. Participar de reuniões técnicas e não técnicas que possuam relevância para a área de Segurança da Informação.

11.1.14. Propor, analisar e implementar ações de hardening;

11.1.15. Manter base de conhecimento de procedimentos técnicos atualizada;

11.1.16. Acompanhar fornecedores quando necessário;

11.1.17. Configuração e operação dos elementos que constituem o sistema de Firewall fornecido pela CONTRATADA, bem como aos demais existentes na CPTM, totalizando 06 (seis) equipamentos, conforme informados no item 1 DESCRIÇÃO DO AMBIENTE DE TI; contemplando:

11.1.17.1. Realização de backup lógico das configurações de Firewall;

11.1.17.2. Gestão de credenciais de acesso ao Firewall;

11.1.17.3. Criação, alteração ou exclusão de configurações definidas e autorizadas pela CPTM:

11.1.17.3.1. Regras de Firewall;

11.1.17.3.2. Perfis de acesso à Internet;

11.1.17.3.3. Perfis de acesso VPN.

11.1.17.4. Análise de logs e eventos gerados pelo Firewall;

11.1.17.5. Aplicação de patches de correção e segurança

11.1.17.6. Suporte e diagnóstico em conjunto com outras equipes para assuntos que envolvam configurações ou ajustes no Firewall;

11.1.17.7. Acompanhamento das ocorrências, aplicação de contramedidas e comunicação ao CPTM sobre tentativas de invasão detectadas no Firewall;

11.1.17.8. Elaboração de relatórios com informações sobre atividades realizadas e indicadores relacionados aos componentes que compõem o sistema de Firewall;

11.1.17.9. O serviço de monitoramento deverá estar disponível em período integral (24 horas × 7 dias por semana), serão aceitos serviços prestados remotamente;

11.1.17.10. O serviço de gerenciamento deverá estar disponível de segunda a sexta-feira, entre 07:00hs e 19:00hs.

12. SOLUÇÃO DE FIREWALL UTM

Os firewalls de próxima geração (NGFW - Next-Generation Firewall) são dispositivos de segurança de rede que oferecem funcionalidades avançadas além do controle de acesso de rede.

A CONTRATADA deverá manter 2 (dois) equipamentos Firewall - Unified Threat Management (NGFW) de igual ou superior capacidade aos existentes contratado como serviço na modalidade On-Site, 24x7, com o seguinte escopo:

12.1.1. VPN

12.1.2. IDS/IPS

12.1.3. Filtro de Conteúdo e acesso à internet

12.1.4. Gerenciamento, análise de log e relatórios

12.1.5. Os equipamentos fornecidos deverão estar licenciados em sua totalidade para os serviços requeridos: firewall de borda, VPN, IDS/IPS, filtro de conteúdo, gerenciamento, análise de logs e emissão de relatórios;

12.1.6. A contratada terá 30 dias após a emissão de ordem de serviço para execução das atividades para disponibilizar, instalar e configurar os equipamentos de firewall.

12.1.7. Ao término do contrato a CONTRATADA deverá retirar do ambiente da CPTM os Firewalls fornecidos para atendimento ao serviço de segurança.

12.1.8. A Solução de Firewall UTM deve ser composta de 02 (dois) appliances de firewall com gerenciamento unificado de ameaças (UTM – unified threat management) e idênticos. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta.

12.1.9. A solução ofertada deve ser de um único fabricante para todos os FIREWALLS UTM, especificados no presente documento, para facilitar o gerenciamento.

12.1.10. Deve implementar alta disponibilidade (HA - high-availability) operando em modo ativo/passivo e ativo/ativo com divisão de carga, sem perdas de conexões. Todas as licenças de software necessárias devem estar habilitadas para esta funcionalidade.

12.1.11. Não serão aceitas soluções de cluster (HA) que necessita reinicializar o(s) equipamento(s) após modificação de parâmetro/configuração.

12.1.12. Deve implementar em um único dispositivo, de forma integrada, tecnologia de firewall stateful packet inspection com capacidade de inspeção por técnica DPI (deep packet inspection), IPS (intrusion prevention system), VPN (virtual private network), gateway antivírus/antispyware e filtro de conteúdo web.

12.1.13. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

12.1.14. Ter suporte aos protocolos TCP, UDP e ICMP;

12.1.15. Ter suporte ao protocolo IPv6;

12.1.16. A solução deve suportar, no mínimo, 400.000 (quatrocentos mil) sessões concorrentes e simultâneas;

12.1.17. A solução deve ser projetada para alta disponibilidade;

12.1.18. Deverá operar em cluster no modo “ativo/ativo” possibilitando a distribuição de carga entre vários links de comunicação e ao mesmo tempo atuando como agentes de contingência entre eles, possibilitando o chaveamento automático de conexões ativas em casos de falhas críticas em um dos equipamentos;

12.1.19. Deverá disponibilizar informações de logs de forma consolidada e centralizada com opção de visualização específica sobre o dispositivo de firewall;

12.1.20. Deverá possibilitar a configuração de regras específicas do cliente, através de solicitação por chamado técnico;

12.1.21. A solução não deve ter restrição de número de usuários simultâneos;

12.1.22. A solução deve permitir a “randomização” do número de sequência TCP, ou seja, funcionar como um “proxy” de número de sequência TCP de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;

12.1.23. Baseado em hardware, não podendo ser Linux Box.

12.1.24. Possuir proteção contra exploração de buffer overflow;

12.1.25. Possuir proteção contra-ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;

12.1.26. Possuir funcionalidades de SSL VPN para no mínimo 500 usuários simultâneos;

12.1.27. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

12.1.28. Possibilidade de agendar a ativação da regra;

12.1.29. Possibilidade de criar regras diferenciadas por aplicações;

12.1.30. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;

12.1.31. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;

12.1.32. Permitir criação de zona confiável, possibilitando que determinados IP's, protocolos ou aplicações se comuniquem na rede;

12.1.33. Gerenciamento integrado a console de gerência da solução;

12.1.34. Capacidade de controle e proteção contra SPIM (Instant Message Spam) e vírus em tráfego de Instant Messaging com suporte a:

12.1.35. WhatsApp;

12.1.36. Signal;

12.1.37. Slack;

12.1.38. Microsoft Teams;

VIRTUAL PRIVATE NETWORK - VPN

12.1.39. A Solução de Firewall UTM deverá ser capaz de realizar as funções de VPN. A solução a ser oferecida pela CONTRATADA deverá ter as seguintes funcionalidades mínimas:

12.1.39.1. Deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança;

12.1.39.2. Deve possuir a capacidade de criação de pools de endereços IP de VPN (endereços privados);

12.1.39.3. Deve permitir a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;

12.1.39.4. Deve possibilitar a visualização do número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas;

12.1.39.5. Para SSL VPN devem ser suportadas no mínimo as seguintes aplicações transportadas sobre conexões SSL para o concentrador: HTTP, POP3S, IMAP4S, SMTPS;

12.1.39.6. Para SSL VPN devem ser suportados, via "Port Forwarding", no mínimo as seguintes aplicações: Telnet, SSH, FTP/SFTP over SSH, Windows Terminal Services, Outlook.

12.1.40. Suportar 120 Gbps de throughput de Firewall stateful;

12.1.41. Suportar 19 Gbps de throughput IPS;

12.1.42. Suportar 35 Gbps de throughput de VPN IPSec;

12.1.43. Suportar 12 Gbps de throughput de Inspeção SSL;

12.1.44. Suportar 15 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes e log habilitado:

12.1.45. Firewall;

12.1.46. Controle de aplicação;

12.1.47. IPS e anti-malware;

12.1.48. • Suportar 10 milhões de conexões simultâneas;

12.1.49. • Suportar 600 mil de novas conexões por segundo;

12.1.50. • Suportar sem o uso de licença, 5 mil túneis de VPN IPSec Site-to-Site simultâneos;

12.1.51. • Suportar sem o uso de licença, 2 mil túneis de clientes VPN IPSec simultâneos;

12.1.52. • Suportar sem o uso de licença, 2 mil clientes de VPN SSL simultâneos;

12.1.53. • Possuir 14 (quatorze) interfaces RJ45 1 Gigabit Ethernet;

12.1.54. • Possuir 10 (dez) interfaces SFP 1 Gigabit Ethernet;

12.1.55. • Possuir 10 (dez) interfaces SFP+ 10 Gigabit Ethernet;

12.1.56. • Possuir 4 (quatro) interfaces QSFP+ 40 Gigabit Ethernet;

12.1.57. • Licenciado e incluído sem custo adicional, 10 sistemas virtuais lógicos por equipamento.

12.1.58.

12.1.59. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN;

12.1.60. • Possuir fonte de alimentação 100-240V AC, 50-60Hz redundante Hot Swappable;

12.1.61.

12.1.62. Licenciado, caso seja necessário, para alta disponibilidade do tipo ativo-passivo, ativo-ativo e clustering para até quatro dispositivos idênticos (hardware e software);

DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS/IPS)

12.1.63. A Solução de Firewall UTM deverá ser capaz de realizar funções de IDS/IPS. A solução a ser oferecida pela CONTRATADA deverá ter as seguintes funcionalidades mínimas:

12.1.63.1. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;

12.1.63.2. Deverá possuir IPS nos níveis de borda de rede, com gerenciamento ativo e características de interações automatizas com sistemas de firewall;

12.1.63.3. Deverá possuir tecnologia IDS / IPS ativo que permita o monitoramento de comportamento malicioso e impeça que ele ocorra, e ao mesmo tempo permitindo o tráfego normal;

12.1.63.4. O sistema IDS / IPS deve ser capaz de detectar, registrar e, se possível prevenir ou retardar ataques como os da

Internet, vetores de ataque malicioso, in-bound e out-bound de tráfego, que apresenta um comportamento mal-intencionado, mas que não é um ataque conhecido ou quaisquer ataques;

12.1.63.5. Bloqueio de ataques baseado na exploração da vulnerabilidade;

12.1.63.6. Deve ser capaz de atuar em modo inline e promiscuous;

12.1.63.7. Capaz de suportar criação de diferentes perfis para acesso ao sistema de IPS;

12.1.63.8. Capacidade de customização dos parâmetros específicos a cada assinatura;

12.1.63.9. Capacidade de realizar shunning para um tráfego pré-determinado;

12.1.63.10. Capacidade de visualização dos logs no próprio sistema através de interface gráfica;

12.1.63.11. O sistema de prevenção à invasão deve suportar a customização das respostas aos ataques detectados;

12.1.63.12. Deve utilizar assinaturas construídas com base em informações de vulnerabilidade e não somente em “exploits” específicos;

12.1.63.13. Deve possuir detecção de anomalias de tráfego da Rede (anomalias associadas a definições estatísticas de tráfego);

12.1.63.14. Deve possuir verificação de adequação dos protocolos que trafegam na rede às definições destes constantes nas RFCs (análise de “RFC compliance”);

12.1.63.15. Deve detectar ataques associados a protocolos que não estejam usando as portas canônicas de serviço (portas padrão reservadas para os protocolos de aplicação);

12.1.63.16. Devem ser suportados no mínimo os seguintes tipos de reação (configuráveis por assinatura de ataque): geração de alerta, gerar trap SNMP, log dos pacotes gerados pelo sistema “vítima”, log dos pacotes gerados pelo sistema que está efetuando o ataque, promover “reset” da conexão TCP, bloquear o pedido de conexão, bloquear o endereço que está gerando o ataque de conexão, negar “in-line” os pacotes associados ao ataque;

12.1.63.17. Deve possuir capacidade de bloquear tráfego “peer-to-peer”;

12.1.63.18. Deve possuir capacidade de bloquear tráfego de “instant messaging”;

12.1.63.19. Deverá possuir tecnologia que agregue e correlacione informações de segurança e que permita o monitoramento de segurança do perímetro de segurança e DMZ, a partir de uma perspectiva central;

12.1.63.20. Deverá possuir tecnologia que permita um melhor gerenciamento dos riscos do negócio.

FILTRO DE CONTEÚDO E CONTROLE DO ACESSO WEB À INTERNET

12.1.64. A Solução de Firewall UTM deverá garantir proteção contra ameaças da Web, objetivando a proteção da interligação da CPTM e a Internet. A solução a ser oferecida pela CONTRATADA deverá ter as seguintes funcionalidades mínimas:

12.1.65. A CONTRATADA deverá fornecer, implantar e operar uma solução de acordo com as especificações descritas neste documento. Deve ser totalmente compatível com virtualização de servidores e microcomputadores, os quais utilizam a solução da VMware;

12.1.66. A CONTRATADA deverá fazer a gestão da solução incluindo:

12.1.66.1.1. Configuração e a gestão de mudanças das políticas informadas pela CPTM;

12.1.66.1.2. Gestão dos backups das políticas de configuração;

12.1.66.1.3. As políticas implementadas poderão ser revistas a pedido da CPTM;

12.1.66.1.4. A Gestão de Capacidade da plataforma será de inteira responsabilidade da CONTRATADA. A solução não deverá requerer nenhum custo de evolução da plataforma, que deverá ser escalável de acordo com a necessidade da CPTM;

12.1.66.1.5. Proteção dinâmica e com roteiros contra malware da Web. O exame de segurança em tempo real, oferecendo proteção contra-ataques baseados em arquivos legados, roteiros da Web e ameaças dinâmicas que contornam os antivírus tradicionais;

12.1.66.1.6. A classificação de conteúdo em tempo real fornecida pela solução, de forma a remover conteúdo inadequado de sites complexos, dinâmicos e protegidos por senha da Web 2.0 que não podem ser classificados com precisão por filtragem tradicional de URL’s;

12.1.66.1.7. Proporcionar o menor custo total de propriedade (TCO), através de segurança de conteúdo consolidada, de forma a reduzir o número de appliances, sistemas de administração em na CPTM;

12.1.66.1.8. Filtro de acessos à Web baseado em listas de URL’s;

12.1.66.1.9. As URL’s devem estar classificadas por categorias e todas as categorias devem ser configuradas para bloquear ou permitir o acesso, bem como permitir o acesso com quotas de tempo, ou permitir o acesso

depois que o usuário aceitar um termo de responsabilidade online;

12.1.67. Deverá possuir políticas por categorias;

12.1.67.1. Deverá analisar o texto dos sítios desconhecidos ou dinâmicos, tanto HTTP quanto HTTPS, filtrando os acessos de acordo com o conteúdo corrente e não apenas a URL, para garantir precisão;

12.1.67.2. Deverá analisar o texto dos sítios Web 2.0 e de Redes Sociais para determinar o conteúdo real e filtrar de acordo com a política de acessos, garantindo granularidade no controle a esses tipos de sítios;

12.1.67.3. Deverá analisar links presentes nos sítes durante a análise de conteúdo, para assim, garantir que um site que possua links para outros com conteúdo indesejável ou malicioso não seja acessado;

12.1.67.4. Deverá realizar uma verificação em busca de códigos maliciosos presentes no conteúdo da página para todos os acessos HTTP e HTTPS ou apenas um grupo específico de sítios;

12.1.67.5. A verificação de segurança do conteúdo dos sítios deve conseguir decodificar e detectar códigos maliciosos dentro de aplicações;

12.1.67.6. Deverá realizar uma varredura nos arquivos binários presentes nos sítios acessados, para garantir que arquivos maliciosos sejam bloqueados;

12.1.67.7. Deverá garantir que, além das atualizações diárias pré-programadas, novas páginas cujo conteúdo represente riscos à segurança sejam adicionadas automaticamente à lista de URL’s alguns minutos depois de haver sido descobertas pelo fabricante da solução, sem necessidade de interação

humana, e sem ter que aguardar pelo horário pré-determinado de atualização da base;

12.1.67.8. Deverá enviar automaticamente para o fabricante da solução, sem intervenção humana, informação sobre todas as URL's não categorizadas que tenham sido acessadas durante o dia pelos funcionários da CPTM, para fins de categorização na base de URL's.

12.1.67.9. Deverá permitir a recategorização manual de qualquer página Web segundo as necessidades da CPTM, bem como permitir que certas páginas possam ser acessadas a qualquer momento mesmo que pertençam a categorias bloqueadas, através de determinação da CPTM;

12.1.67.10. Deverá permitir que se incluam manualmente URL's ou Expressões Regulares, para que certas páginas sejam tratadas diferentemente da categorização original do fabricante da solução;

12.1.67.11. Deverá permitir o bloqueio de páginas que pertençam a categorias permitidas, mas cuja URL possua certas palavras-chave;

12.1.67.12. Deverá permitir o acesso a páginas de certas categorias, mas bloquear acesso a certos tipos de arquivos dentro dessas páginas (tais como vídeo, áudio, arquivos compactados, executáveis, documentos.);

12.1.67.13. Os tipos de arquivos deverão permitir a customização por tipo de extensão do arquivo, bem como a criação de novos tipos de arquivos, mesmo que não sejam normalmente encontrados na Internet;

12.1.68. Deverá permitir a definição de políticas por IP, faixas de IP's, usuários e grupos do seguinte serviço de diretório:

12.1.68.1. Domínios do Microsoft Active Directory;

12.1.69. Deverá reconhecer de forma transparente os usuários seguintes:

12.1.69.1. Usuários de Active Directory;

12.1.69.2. Usuários LDAP autenticados por RADIUS.

12.1.70. Deverá permitir que o administrador selecione tipos de autenticação diferentes para os usuários da mesma rede, ou seja, que determinado grupo de usuários seja autenticado manualmente e o restante seja autenticado de forma transparente;

12.1.71. Deverá pedir autenticação manual para usuários que tentem navegar sem estar devidamente autenticados no serviço de diretório, sem pedir autenticação manual aos usuários que já foram autenticados no domínio;

12.1.72. Deverá permitir a definição de uma política geral que se aplique aos usuários que não tenha uma política específica assignada;

12.1.73. Deverá permitir diferentes tipos de bloqueio por horários do dia e dias da semana para qualquer das políticas definidas;

12.1.74. Deverá permitir a definição de quotas de tempo diferentes para usuários de grupos diferentes, para usuários específicos e para os usuários em geral;

12.1.75. Deverá exibir uma página HTML customizável cada vez que um usuário tentar acessar uma página bloqueada;

12.1.76. Deverá pedir confirmação ao usuário cada vez que seja necessário usar sua quota de tempo para navegar em qualquer página que pertença a uma categoria que tenha sido definida como permitida com o uso das quotas de tempo através de uma página HTML customizável;

12.1.77. Filtro de protocolos não HTTP baseado em listas de protocolos:

12.1.77.1. Deverá possuir lista de protocolos utilizados na filtragem;

12.1.77.2. Deverá possuir a capacidade de bloquear os protocolos segundo as políticas definidas;

12.1.78. Deverá permitir a definição de políticas específicas de uso de mensagens instantâneas, de modo que: determinados usuários possam utilizá-las livremente; outros tenham seu uso completamente bloqueado; e um terceiro grupo possa utilizá-las apenas para comunicação por texto, com o envio e recebimento de arquivos anexos devidamente bloqueados.;

12.1.79. Deverá exibir uma mensagem de bloqueio ao usuário cada vez que haja uma tentativa de acessar um protocolo bloqueado;

12.1.80. Proxy Web:

12.1.80.1. Possuir a funcionalidade de Proxy Web, suportando os protocolos HTTP, HTTPS, FTP e SFTP;

12.1.80.2. Deverá permitir a configuração das portas usadas para cada um dos protocolos suportados;

12.1.80.3. Deverá ser capaz de atuar como um proxy explícito e transparente simultaneamente;

12.1.80.4. Deverá criar e hospedar arquivos PAC (Proxy Auto Configuration) e WPAD (Web Proxy Auto Discovery);

12.1.81. Deverá possuir a capacidade de autenticar usuários através dos seguintes protocolos:

12.1.81.1. Kerberos;

12.1.81.2. NTLM;

12.1.81.3. Radius;

12.1.81.4. LDAP.

12.1.82. Permitir a configuração de dois ou mais protocolos para autenticar usuários, sendo um para cada subrede distinta;

12.1.83. Deverá permitir a criação de backups da configuração, salvando-os localmente ou em servidor remoto;

12.1.83.1. Deverá permitir ser um membro de uma hierarquia de cache HTTP e ICP (Internet Cache Protocol);

12.1.83.2. Deverá suportar o armazenamento de conteúdo em cache;

12.1.83.3. Deverá possuir mecanismo para decriptação do tráfego SSL para fins de inspeção do conteúdo HTTPS acessado;

12.1.83.4. Permitir a configuração de categorias ou sites isolados para que o tráfego SSL não seja descriptografado.

GERENCIAMENTO, ANÁLISE DE LOGS E EMISSÃO DE RELATÓRIOS

12.1.84. Deverá ser fornecido sistema de gerenciamento centralizado da solução de Firewalls UTM composto de 2 (dois) ou mais equipamentos (hardware e software) implementados em configuração redundante para alta disponibilidade, para gerenciamento, análise de logs e emissão de relatórios;

12.1.85. O modelo ofertado do sistema de gerenciamento (hardware e software) deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta;

12.1.86. Os equipamentos devem ser novos e sem uso anterior;

12.1.87. O sistema de gerenciamento deve ser do mesmo fabricante da solução de Firewalls UTM a serem fornecidos;

12.1.88. A CONTRATADA deve fornecer licenças de uso de todos os softwares que compõem a Solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta;

12.1.89. Fornecer, caso necessário, sistema gerenciador de banco de dados relacional para armazenar os logs de eventos gerados pelos firewalls;

12.1.90. Cada appliance ou servidor deve possuir no mínimo 4.0 TB de disponibilidade de armazenamento em disco;

12.1.91. Os discos de armazenamento devem possuir redundância em RAID 1, RAID 5 ou RAID 10;

12.1.92. Instalar programas para monitorar o tráfego do ambiente de TI e registrar as tentativas de ataques (internos e externos), apresentando relatórios nativos da Solução de Firewall UTM, mensais da gestão efetuada e as ocorrências verificadas;

12.1.93. Permitir a classificação dos elementos de segurança em grupos e, então, aplicar políticas de segurança específicas ao grupo, sendo que a distribuição destas políticas é feita de forma automática pelo sistema de gerenciamento. O sistema também deve permitir a criação e aplicação de regras globais de segurança;

12.1.94. Interface amigável (web ou não), que permita executar as ações de configuração e monitoração dos equipamentos e políticas de segurança (tabelas, gráficos, janelas);

12.1.95. Acompanhamento e implementação de usuários, grupos de usuários, definição de políticas de acesso e monitoração do acesso;

12.1.96. Acompanhamento e implementação de operações tais como backup de configurações (regras), aplicação de patches e novas atualizações de software, gerenciamento de modificações e análise de logs;

12.1.97. Monitoração do firewall em tempo real, de alertas de invasões, de análise de tráfego atípico, detecção de scans, spoofing, tentativas de autenticação fracassadas, Denials of Service (DoS);

12.1.98. Ações corretivas, relacionadas a eventos de emergência, tais como falhas no firewall, possíveis intrusões que comprometam a política de segurança da empresa, ou ainda uma não resposta do firewall;

12.1.99. A CONTRATADA deverá fazer a gestão solução, administrando atualizações de vacinas, patchs ou sistema operacional nos elementos que compõem a solução ofertada à CPTM;

12.1.100. A CONTRATADA deverá realizar a emissão de relatórios de acordo com o previsto na tabela de SLA, de acordo com os modelos previamente estabelecidos e acordados entre CONTRATANTE e CONTRATADA;

12.1.101. Visualização do status atual dos firewalls, tarefas pendentes e mensagens de log de forma central em tempo real, além dos relatórios gráficos dos firewalls e atividades da rede por firewall;

12.1.102. Fornecimento de relatórios gráficos do firewall e atividades de rede, além de dados históricos e em tempo real, oferecendo uma visão das ocorrências na rede;

12.1.103. Monitoração de processos em tempo real, ou seja, da utilização da unidade central de processamento (CPU) do firewall e de processos, com informação de valores correntes e totais;

12.1.104. Monitoração, em tempo real, dos tráfegos detectados como: acessos web, aplicações, IPS, vírus, spyware e VPN;

12.1.105. Fornecimento dos seguintes relatórios em formato HTML ou PDF: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias web mais acessadas, maiores emissores e receptores de e-mail;

12.1.106. Fornecimento dos seguintes relatórios com cruzamento de informações: máquinas acessadas x serviços bloqueados, usuários x URLs acessadas, usuários x categorias web bloqueadas;

12.1.107. A CONTRATADA deverá realizar a entrega relatórios sob demanda solicitados formalmente pela contratada. Estes relatórios serão de estudo, aprofundamento em incidentes, correlacionamentos de eventos, ou assuntos similares;

12.1.108. Deverá possuir serviço de armazenamento de registros de log;

12.1.109. Deverá permitir que certas categorias de URL's não gerem logs para fins de diminuição do volume de logs armazenados;

12.1.110. Deverá fazer o roll-over da base de dados de logs cada vez que for atingido um tamanho predeterminado, ou bem por períodos de dias configurados pelo administrador, sem interrupção do armazenamento e sem a necessidade de interação humana;

12.1.111. Deverá excluir automaticamente bases de dados históricas quando seu conteúdo for mais antigo que uma quantidade determinada de dias definido pelo administrador;

12.1.112. Deverá ser capaz de gerar relatórios gráficos baseados em modelos pré-definidos nativos da solução, os quais deverão permitir filtro por usuários, grupos de usuários, protocolos, categorias e bloqueios;

12.1.113. Deverá gerar relatórios nos formatos PDF e HTML**;**

12.1.114. Deverá permitir a programação de múltiplas tarefas de geração de relatórios pré-determinados, em horários e dias da semana pré-definidos, e deverá enviar os relatórios gerados por correio eletrônico para os destinatários desejados;

12.1.115. Deverá possuir interface de monitoramento dos acessos à Internet em tempo real, sendo possível pausar para revisar a atividade de filtragem corrente;

12.1.116. Deverá possuir interface de acesso direto aos registros de log utilizando o conceito de drill-down;

12.1.117. Deverá permitir a geração automática de relatórios e sua distribuição por correio eletrônico para os destinatários desejados.

12.1.118. Implementação e Administração:

12.1.118.1. A solução deverá possuir funcionalidade de gerenciamento Web para administração e geração de relatórios;

12.1.118.2. A interface de gerenciamento Web deverá possuir um painel que apresente o estado corrente da solução e ilustre graficamente a atividade de filtragem dos acessos do dia;

12.1.118.3. A interface de gerenciamento Web deverá mostrar, através de um painel, uma visão geral da atividade de filtragem dos acessos dos últimos 30 dias, atualizando os dados diariamente;

12.1.118.4. Deverá permitir a criação de administradores delegados, definindo permissões administrativas, permissões para geração de relatórios e auditores do sistema;

12.1.118.5. Deverá permitir múltiplos logins de administradores delegados simultaneamente;

12.1.118.6. Deverá integrar-se ao AD para que o acesso dos administradores a console de gerenciamento ocorra através do uso da conta e senha do usuário no AD;

12.1.118.7. Deverá permitir que usuários do AD que não possuam direitos de Administradores do Domínio possam ser designados como Administradores da solução;

12.1.119. Deverá manter registro para fins de auditoria de cada modificação feita por cada Super Administrador ou Administrador Delegado nas políticas e configurações da solução.

13. SOLUÇÃO DE SEGURANÇA DE ENDPOINTS E REDE

CARACTERISTICAS GERAIS

13.1.1. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos, mesmo que estejam compactados pelas ferramentas de mercado, tendo como abrangência até o 6º (sexto) nível de compactação;

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

13.1.3. A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin, execução de arquivo ou módulo adicional;

13.1.4. Instalação e atualização da solução sem a intervenção do usuário;

13.1.5. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente por senha;

13.1.6. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;

13.1.7. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança.

13.1.8. Apresentar relatórios mensais com as ocorrências registradas e/ou observadas.

13.1.9. Todas as funcionalidades descritas devem estar devidamente licenciadas para utilização durante todo o período contratual.

13.1.10. Possuir console Web para gerenciamento e administração da ferramenta;

13.1.11. A solução deverá ser toda de um único fabricante;

13.1.12. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente.

13.1.13. Deve possuir módulo de proteção Anti-Malware

13.1.14. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais em uso na CPTM:

13.1.15. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

13.1.16. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

13.1.17. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

13.1.17.1. Processos em execução em memória principal (RAM);

13.1.17.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

13.1.17.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

13.1.17.4. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

13.1.17.5. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;

13.1.18. Deve possuir detecção heurística de vírus desconhecidos;

13.1.19. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

13.1.20. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

13.1.20.1. Em tempo real de arquivos acessados pelo usuário;

13.1.20.1.1. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

13.1.20.1.2. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

13.1.20.2. Automáticos do sistema com as seguintes opções:

13.1.20.2.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

13.1.20.2.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

13.1.20.2.3. Frequência: horária, diária, semanal e mensal;

13.1.20.3. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

13.1.21. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

13.1.22. Em caso de arquivos suspeitos, a solução deve ter a capacidade de enviar o artefato para um ambiente de sandbox do próprio fabricante para identificar ameaças desconhecidas;

13.1.23. O módulo de análise de artefatos desconhecidos (sandbox) deve estar integrada à solução de antimalware, sem necessidade de plugins adicionais;

13.1.24. O módulo de sandbox deve permitir a análise de arquivos submetidos diretamente dos agentes;

13.1.25. Em caso de ameaças desconhecidas detectadas pela sandbox, a solução deve ter a capacidade de adicionar os objetos suspeitos (hash de arquivo, IP, domínio e URL) numa lista de bloqueio automaticamente;

13.1.26. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

13.1.27. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

13.1.28. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

13.1.29. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

13.1.30. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

13.1.31. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos

13.1.32. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

13.1.33. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

13.1.34. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

13.1.35. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

13.1.36. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de ofuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

13.1.37. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

13.1.38. Deve bloquear processos comuns associados a ransomware;

13.1.39. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios

13.1.40. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

13.1.41. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

13.1.42. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

13.1.43. Deve permitir atualização incremental da lista de definições de vírus;

13.1.44. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

13.1.45. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

13.1.46. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

13.1.47. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

13.1.48. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

13.1.49. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

13.1.50. Deve possibilitar instalação "silenciosa";

13.1.51. Deve permitir o bloqueio por nome de arquivo;

13.1.52. Deve permitir o travamento de pastas e diretórios;

13.1.53. Deve permitir o travamento de compartilhamentos;

13.1.54. Deve permitir o rastreamento e bloqueio de infecções;

13.1.55. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

13.1.56. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

13.1.57. Deve permitir a desinstalação através da console de gerenciamento da solução;

13.1.58. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

13.1.59. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

13.1.60. Deve permitir a deleção dos arquivos quarentenados;

13.1.61. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

13.1.62. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;

13.1.63. Deve identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada. Em caso de soluções em nuvem, será aceita utilização de ferramenta do próprio fabricante para varredura local;

13.1.64. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

13.1.65. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

13.1.66. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o

download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

13.1.67. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;

13.1.68. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

13.1.69. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

13.1.70. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

13.1.71. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

13.1.72. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;

13.1.73. Deve possuir capacidades de níveis de sensibilidade da solução para os módulos:

13.1.74. Análise de comportamento de ameaças;

13.1.75. Análise com base em aprendizagem de máquina;

13.1.76. Análise de comunicações suspeitas;

13.1.77. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

13.1.78. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

13.1.79. Deve permitir a criação de usuários locais de administração da console de anti-malware;

13.1.80. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

13.1.81. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

13.1.82. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

13.1.83. Deve permitir a gerência de domínios separados para usuários previamente definidos;

13.1.84. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

13.1.85. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

13.1.86. Deve possuir módulo de Controle de Dispositivos

13.1.87. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

13.1.88. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

13.1.89. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções:

acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

13.1.90. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

13.1.91. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

13.1.92. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

13.1.93. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

13.1.94. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

13.1.95. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

13.1.96. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

13.1.97. Deve prover funcionalidade de HIPS – Host IPS e Host Firewall

13.1.98. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais em uso na CPTM:

13.1.99. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

13.1.100. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

13.1.101. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

13.1.102. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

13.1.103. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

13.1.104. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

13.1.105. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

13.1.106. O modulo de HIPS deverá possuir regras para proteger contra ameaças do tipo Ransomware;

13.1.107. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

13.1.108. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

13.1.109. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

13.1.110. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

13.1.111. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

13.1.112. Deve possuir módulo para Controle De Aplicações

13.1.113. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais em uso na CONTRATANTE:

13.1.114. As regras de controle de aplicação devem permitir as seguintes ações:

13.1.114.1. Permissão de execução;

13.1.114.2. Bloqueio de execução;

13.1.114.3. Bloqueio de novas instalações.

13.1.115. A regra de liberação para o controle de aplicação deverá pemitir que o programa liberado efetue ou não a execução de outros processos,

13.1.116. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

13.1.117. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

13.1.117.1. Assinatura SHA-1 e SHA-256 do executável;

13.1.117.2. Atributos do certificado utilizado para assinatura digital do executável;

13.1.117.3. Caminho lógico do executável;

13.1.117.4. Base de assinaturas de certificados digitais válidos e seguros.

13.1.118. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

13.1.119. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

13.1.120. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

13.1.121. Deve permitir a busca por aplicações ou fabricante destas;

13.1.122. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

13.1.123. Deve possuir módulo integrado de Detecção e Resposta

13.1.124. A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

13.1.125. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

13.1.126. A solução deve possuir módulo de investigação e detecção integrados;

13.1.127. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

13.1.128. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

13.1.129. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

13.1.130. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

13.1.131. Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

13.1.132. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

13.1.133. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

13.1.134. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

13.1.135. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

13.1.136. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

13.1.137. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

13.1.138. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

13.1.139. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

13.1.140. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

13.1.141. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

13.1.142. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

13.1.143. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

13.1.144. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

13.1.145. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

13.1.146. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

13.1.147. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

13.1.148. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

13.1.149. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

13.1.150. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

13.1.151. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

13.1.152. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

13.1.153. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

13.1.154. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

13.1.155. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

13.1.156. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

13.1.157. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

13.1.158. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

13.1.159. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

13.1.160. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

13.1.161. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

13.1.162. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

13.1.163. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

13.1.164. Restaurar a conectividade da estação de trabalho com a rede;

13.1.165. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

13.1.166. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

SOLUÇÃO DE INSPEÇÃO DE REDE CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA

13.1.167. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CPTM, inspecionando o tráfego de rede, independente de agentes instalados;

13.1.168. O sensor avançado de análise de rede deve ser licenciado a fim de inspecionar o Throughput total informado pela CPTM;

13.1.169. Deve atuar com a inspeção de rede da CPTM, estendendo visibilidade sob tráfego leste-oeste e norte-sul;

13.1.170. O Sensor deve ser instalado de modo a detectar ameaças avançadas no ambiente da CPTM, inspecionando o tráfego de rede, independente de agentes instalados;

13.1.171. O sensor deve ser instalado a fim de detectar ameaças avançadas no ambiente da CPTM, inspecionando o tráfego de rede, independente de agentes instalados;

13.1.172. O sensor deve aplicar técnicas de análise de tráfego avançadas baseadas em aprendizagem de máquina;

13.1.173. O sensor deve atuar com técnicas de detecção e resposta específicos para modelos de detecção focados em rede, de forma a identificar comportamentos maliciosos;

13.1.174. O sensor deve permitir que seja implantado em linha com o tráfego de rede e em modo de espelhamento de rede;

13.1.175. Caso seja implementada em linha na rede da CPTM, o sensor deve permitir a criação de regras de by-pass para casos de falhas de interface;

13.1.176. Deve suportar o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

13.1.177. Durante a inspeção do tráfego de rede em tempo real, o sensor deverá ser capaz de identificar anomalias na rede e gerar alertas em casos de tráfego suspeito;

13.1.178. Deve implementar características de Network Detection and Response baseado em comportamento;

13.1.179. Quando implantada em linha com a rede da CPTM, o sensor deve ter a capacidade de analisar tráfego TLS, sem necessidade de licenciamento adicional;

13.1.180. Deve identificar ameaças direcionadas avançadas e persistentes (APT);

13.1.181. Deve analisar possíveis fases de um ataque direcionado, identificando tentativas de coletas de informação, movimentação lateral, exfiltração de dados, descoberta de dispositivos e comunicações de comando e controle (C&C);

13.1.182. Deve identificar e mapear possíveis pontos de entrada na rede que possam ser exploradas por atacantes;

13.1.183. Deve prover automatizações para bloqueio de ameaças identificadas a partir da inspeção de rede;

13.1.184. O Sensor de inspecionar a rede a fim de analisar, no mínimo os protocolos: HTTP, HTTPS, LDAP, FTP, Telnet, WebSocket, SMTP, POP3, DNS, SMB, RDP, Kerberos, IRC, VNC, SQL, MYSQL e ARP.

13.1.185. Deve permitir análise de arquivos em sandbox, permitindo identificar ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, vulnerabilidades conhecidas e arquivos maliciosos no tráfego de rede, de forma automática e quando aplicável;

13.1.186. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos executáveis (scripts), PDF´s, executáveis, PPTX, DOCX, XLSX, LNK, ELF, CHM, RTF, ODP, DLLs, JAR, ZIP e RAR;

13.1.187. O sensor de inspeção de rede, deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Linux nas distribuições (CentOS), Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019;

13.1.188. Deve suportar a criação de sandboxes que repliquem os sistemas operacionais e aplicações da CPTM, para avaliação do real impacto da ameaça no ambiente;

13.1.189. Possibilitar a predefinição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;

13.1.190. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em único ponto;

13.1.191. Deve possuir atualização automática de regras, sendo que estas devem ser disponibilizadas via internet pelo fabricante da solução;

13.1.192. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

13.1.193. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

13.1.194. Deve possuir interface web para busca e investigação local de incidentes;

13.1.195. Capacidade de detectar ameaças web derivadas de vulnerabilidades e downloads de conteúdo malicioso;

13.1.196. Não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede;

13.1.197. A solução deve ser capaz de analisar protocolos mascarados ou tunelados em ICMP, IP, UDP e TCP;

13.1.198. Deve ser capaz de detectar ameaças desconhecidas, ataques dirigidos e ameaças de dia zero, sendo que este módulo majoritariamente deve pertencer ao mesmo fabricante;

13.1.199. Deve permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo, múltiplas camadas de empacotamento e arquivos comprimidos;

13.1.200. Deve suportar o monitoramento de múltiplas interfaces de rede conectadas a diferentes VLANs e Switches;

13.1.201. Deve permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

13.1.202. Deve possibilitar que modelos de detecção a nível de rede sejam customizados de acordo com as necessidades da CPTM;

13.1.203. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e escaneamentos de porta;

13.1.204. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de Servidor SMTP não autorizado e Servidor Proxy não autorizado;

13.1.205. Deve possuir regras que identifiquem comunicações streaming de mídia, peer-to-peer e instant messengers;

13.1.206. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

13.1.206.1. Sumário das detecções;

13.1.206.2. Visão Geral dos Incidentes de Segurança;

13.1.206.3. Discriminação dos Tipos de Incidentes;

13.1.206.4. Top Ameaças Analisadas;

13.1.206.5. Top Hosts Infectados;

13.1.206.6. Recomendações de Segurança;

13.1.206.7. Executivos;

13.1.206.8. Deve possuir detalhes técnicos dos incidentes detectados;

13.1.206.9. Deve possuir estatística do tráfego analisado;

13.1.206.10. Deve possuir indicadores de risco do ambiente;

13.1.206.11. Recomendações de Segurança.

13.1.207. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e atualizada dinamicamente, hosts com alto nível de risco, classificando os tipos de eventos detectados;

13.1.208. Deve permitir o upgrade e downgrade de versão de firmware;

13.1.209. Deve ser capaz de identificar ameaças que afetam dispositivos móveis, especificamente aqueles baseados em IOS e Android;

13.1.210. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns e tunelamento de protocolo;

13.1.211. Deve ser capaz de detectar tentativas de escaneamento de rede;

13.1.212. Deve ser capaz de detectar propagação de malwares na rede;

13.1.213. Deve ser capaz de detectar tentativas de força bruta em credenciais;

13.1.214. Deve ser capaz de detectar tentativas de roubo de informação;

13.1.215. Deve ser capaz de detectar ameaças que se replicam na rede;

13.1.216. Deve ser capaz de detectar Exploits na rede;

13.1.217. Deve replicar a comunicação captada por interface gráfica interativa, a fim de facilitar a compreensão dos alertas gerados;

13.1.218. Deve possuir interface gráfica que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas;

13.1.219. Deve apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboard;

13.1.220. Deve permitir busca por informações de destino e origem de comunicações, incluindo: endereço IP, endereço MAC, domínio, protocolo e grupo de rede;

13.1.221. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

13.1.222. Capacidade de salvar uma investigação antes de ser finalizada;

13.1.223. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

13.1.224. Capacidade de gerar relatórios baseados nas investigações;

13.1.225. Deve permitir exportar sob demanda os logs padrões CSV ou PDF;

13.1.226. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

13.1.227. Deve ser totalmente integrado com a console de gerência da plataforma do próprio fabricante, com objetivo de correlacionar as detecções do sensor de rede com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e gateway seguro;

13.1.228. Deverá ser capaz de identificar ameaças evasivas em tempo real atuando com análise profunda e inteligência para identificar e prevenir ataques;

13.1.229. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

13.1.230. O sensor de inspeção de rede deve ter a capacidade de integrar-se com a plataforma de gerência centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

13.1.231. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:

13.1.231.1. Uso de CPU

13.1.231.2. Uso de Disco;

13.1.231.3. Uso de Memória;

13.1.231.4. Tráfego malicioso analisado;

13.1.231.5. Todo o tráfego analisado.

13.1.232. A solução deverá ter integração com ferramentas de SIEM;

13.1.233. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

13.1.234. Deverá suportar ao menos a integração com dois servidores syslogs;

13.1.235. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

13.1.236. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

13.1.237. A solução deve ter capacidade de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;

13.1.238. Deverá listar os 10 hosts mais críticos do ambiente da CPTM, de forma a categorizá-los de acordo com a severidade atual baseada em número e criticidade das detecções, segundo:

13.1.238.1. Nível Crítico

13.1.238.2. Nível Alto

13.1.238.3. Nível Médio

13.1.238.4. Nível Baixo

13.1.239. Deverá correlacionar cada host listado a um alerta de investigação, quando aplicável;

13.1.240. As detecções de cada host listado deverão ser apresentadas com detalhes para devida investigação;

13.1.241. Deverá apresentar os logs de rede de maneira evidente e destaca por meio de rótulo e cor, a fim de diferenciar dos demais logs de outros sensores;

13.1.242. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

13.1.242.1. Computadores infectados;

13.1.242.2. Origem de infecções;

13.1.242.3. Estatísticas de ameaças;

13.1.242.4. Riscos potenciais de segurança;

13.1.242.5. Riscos de perda de informações;

13.1.242.6. Risco de sistema comprometido;

13.1.242.7. Risco de disseminação de ameaças;

13.1.242.8. Infecções de malware

13.1.242.9. Eventos suspeitos;

13.1.243. Deve permitir a configuração de alarmes personalizados, com base em investigações;

13.1.244. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

13.1.245. Deve ser capaz de inspecionar até 1 GBPS na modalidade Virtual e até 4 GBPS na modalidade appliance físico;

13.1.246. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado

13.1.247. A solução deve possuir recurso de prevenção de ameaças avançadas, com capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK MITRE Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução;

13.1.248. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

13.1.249. A partir de um alerta do sensor de rede, deve ser possível o bloqueio dos IPs e URLs envolvidos no contexto da detecção;

13.1.250. Deve mapear os métodos de requisições detectados ao longo de uma comunicação inspecionada, listando ao menos:

13.1.250.1. Requisições GET

13.1.250.2. Requisições POST

13.1.250.3. Requisições MOVED

13.1.250.4. Requisições NOT FOUND

13.1.251. A partir dos alertas gerados, deve correlacionar as máquinas, IPs e Hashs envolvidos, apontando possíveis indicadores de comprometimento (IOCs) ao ambiente da CPTM;

13.1.252. Os relatórios e logs deverão ser exportados nos formatos PDF, TXT ou CSV;

13.1.253. O sensor deve por meio da integração com a plataforma de detecção e resposta, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos: Fortinet, Palo Alto ou Checkpoint;

CONSOLE DE GERENCIAMENTO DA PLATAFORMA DE DETECÇÃO E RESPOSTA ESTENDIDA

13.1.254. A solução deve fornecer uma console única para gerenciamento dos serviços de segurança, integrando-se com os outros componentes;

13.1.255. Capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

13.1.256. A console de administração deverá permitir o envio de notificações via SMTP

13.1.257. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

13.1.258. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

13.1.259. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

13.1.260. Deverá orquestrar todas as funcionalidades descritas;

13.1.261. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

13.1.262. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;

13.1.263. Prover nota de risco para o ambiente de TI da CPTM, baseada em diversos fatores e comparável com a de outras organizações da mesma região, indústria ou tamanho;

13.1.264. Deve suportar integração com os seguintes serviços de diretório:

13.1.264.1. Microsoft Active Directory;

13.1.264.2. Azure Active Directory; Entra ID;

13.1.264.3. Open LDAP;

13.1.264.4. A nota de risco deve ser calculada continuamente e deve ser possível analisar seu comportamento ao longo do tempo de forma gráfica;

13.1.264.5. As fontes de dados para cálculo do risco não devem se limitar àquelas desenvolvidas pelo FABRICANTE, sendo aceitas soluções de terceiros;

13.1.265. Deve prover um sumário dos itens referentes ao escopo de risco cibernético mapeado, apresentando as ações a serem executadas, a fim de diminuir o valor numérico do risco;

13.1.266. Deve apresentar alertas de possíveis comprometimentos de contas;

13.1.267. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

13.1.268. Suporte a atribuição de papéis funcionais, para implantação de política de controle de acesso baseada em papéis (RBAC - Role-based access control);

13.1.269. A console de administração deve metrificar o nível de risco cibernético do ambiente, baseando-se na telemetria gerada pelas demais soluções citadas nos itens 13

13.1.270. Deve mapear as vulnerabilidades existentes nas máquinas, elencando quanto ao nível de CVSS score e impacto no ambiente, apresentando as vulnerabilidades que estão sofrendo algum tipo de exploração a nível das máquinas e da rede;

13.1.271. Deve apontar as vulnerabilidades com o maior índice de risco presentes no ambiente;

13.1.272. Deve apresentar os alertas de ameaças direcionadas, suspeitas, e de dia zero, a fim de identificar possíveis ações maliciosas no ambiente da CPTM;

13.1.273. Tais alertas devem apresentar:

13.1.273.1. A relação entre máquinas e IPs;

13.1.273.2. Requisições de rede;

13.1.273.3. URLs e Hashs;

13.1.273.4. Usuários e domínios;

13.1.274. Deve ser possível customizar os modelos de detecção, a fim de atender as necessidades da CPTM;

13.1.275. Deve ser possível criar exceções para os modelos de detecção;

13.1.276. A solução deve ser baseada em inteligência artificial e aprendizagem de máquina, a fim de potencializar os níveis de detecção de comportamentos anômalos;

13.1.277. Deve possuir rede global de inteligência de ameaças;

13.1.278. Deve apresentar alertas caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais;

13.1.279. Deve possuir módulo de pesquisa forense de ameaças, possibilitando a coleta de logs remotamente;

13.1.280. Deve suportar conexões remotas via agente da solução, sendo possível:

13.1.280.1. Coleta de evidências forenses;

13.1.280.2. Isolar a máquina;

13.1.280.3. Terminar processo;

13.1.280.4. Dump de memória;

13.1.280.5. Listar as portas abertas na máquina;

13.1.280.6. Listar configurações de rede;

13.1.280.7. Listar os diretórios;

13.1.280.8. Deletar arquivo ou diretório;

13.1.281. Enumerar a superfície de ataque da CPTM, dependendo das fontes de dados conectadas, compreendendo:

13.1.281.1. As estações de trabalho, os servidores e os dispositivos móveis da CPTM;

13.1.281.2. Os usuários da CPTM, apontando inclusive aqueles que detêm poderes administrativos;

13.1.281.3. As aplicações acessadas por usuários e dispositivos da CPTM, apontando inclusive aquelas que passaram por recente vazamento de dados;

13.1.281.4. Os ativos mantidos pela CPTM sob custódia de Provedores de Serviços em Nuvem;

13.1.281.5. Os domínios da CPTM, suportando ao menos 10 domínios diferentes;

13.1.281.6. Os subdomínios da CPTM;

13.1.281.7. Os IPs Públicos associados à CPTM e seus respectivos hosts;

13.1.281.8. As portas de comunicação/serviços abertos em cada host público;

13.1.282. Deve mapear via rede da CPTM os dispositivos existentes e apontar aqueles que não são gerenciados pelos agentes da solução;

13.1.283. Deve apresentar a relação de máquinas que o usuário acessou;

13.1.284. Deve listar os alertas identificados no ambiente e correlacionar com técnicas, táticas e procedimentos do framework MITRE ATT&CK;

13.1.285. Tais alertas devem seguir o seguinte escopo de severidade quanto ao nível de risco:

13.1.285.1. Risco Crítico;

13.1.285.2. Risco Alto;

13.1.285.3. Risco Médio;

13.1.285.4. Risco Baixo.

13.1.286. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

13.1.287. Deve haver correlação entre eventos de detecção, a fim de apresentar um possível incidente de segurança;

13.1.288. Deve suportar que o usuário manualmente correlacione alertas em um incidente;

13.1.289. Deve possibilitar que um usuário atribua o alerta a outro usuário;

13.1.290. Deve possuir campo para observações e notas;

13.1.291. Cada alerta deverá ser listado com um status de:

13.1.291.1. Novo alerta;

13.1.291.2. Alerta sendo tratado;

13.1.291.3. Falso Positivo

13.1.291.4. Fechado;

13.1.291.5. Verdadeiro Positivo.

13.1.292. Deve listar todos as ações de resposta executadas, apresentando o status de cada uma;

13.1.293. Deve possuir lista customizável de indicadores de comprometimento (IOC) e objetos suspeitos;

13.1.294. Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;

13.1.295. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos.

13.1.296. Deve informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

13.1.297. A solução deve mostrar, pelo menos, o timestamp e objetos envolvidos (comandos, processos, usuários, servidores);

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

13.1.299. Para a integração com o sensor de inspeção de rede, a solução deverá receber os alertas advindos do sensor de inspeção de rede, processá-los e analisá-los, a fim de identificar os riscos de segurança existentes;

13.1.300. Deve reter os logs gerados pelos sensores de endpoints, rede e e-mails por no mínimo 30 dias;

13.1.301. Com base na telemetria do sensor de inspeção de rede, deverá replicar a sequência de requisições ocorridas dentre as máquinas da rede da CPTM e endereços externos, a fim de apresentar eventos correlacionados para permitir investigações forenses;

13.1.302. Deverá correlacionar os logs do sensor de inspeção de rede e indicar quais vulnerabilidades existentes nas máquinas estão sofrendo tentativas de exploração;

13.1.303. A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deverá ser capaz de disponibilizar as regras de proteção indicadas;

13.1.304. Os eventos de segurança gerados devem ser retidos na plataforma por no mínimo 30 dias para fins de auditoria;

13.1.305. Com base na telemetria gerada, deve apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;

13.1.306. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

13.1.307. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

13.1.308. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

13.1.309. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

13.1.310. Deve ser capaz de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

13.1.311. Capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;

13.1.312. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

13.1.313. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

13.1.314. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

13.1.315. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

13.1.316. Deve ser capaz de correlacionar os logs gerados pelos sensores de rede, e-mail e Endpoint, a fim de gerar um alerta multicamadas;

13.1.317. Deve possibilitar o envio de scripts com base em Powershell e Bash via sensor da solução;

13.1.318. Deve ser possível que sessões de acesso remoto seguro sejam iniciadas via sensor presente nas máquinas;

13.1.319. Deve lista as vulnerabilidades mapeadas de forma a definir quais CVEs, com base no NIST, estão relacionados e ainda, informar se explorações estão sendo vistas nas máquinas;

13.1.320. A partir de um log pesquisado na plataforma, deve ser capaz de criar alertas customizados;

13.1.321. Deve armazenar querys executados na aba de pesquisa da plataforma;

13.1.322. Deve possuir Sandbox que seja capaz de processar e analisar arquivos e URLs;

13.1.323. Deve ter suporte a criação de modelos de detecção customizados, a fim de endereçar casos específicos da CPTM;

13.1.324. Deve ser possível criar modelos de detecção com base em detecções e comportamentos anômalos associados;

13.1.325. Deve prover gateway seguro e privado de comunicação para integração com soluções de Firewall e Escaneadores de vulnerabilidades;

13.1.326. Deve ser capaz de criar fluxos de resposta automatizada, tais como:

13.1.326.1. Isolar uma máquina;

13.1.326.2. Terminar um processo;

13.1.326.3. Rodar um script customizado;

13.1.326.4. Adicionar um objeto suspeito na lista de IOCs;

13.1.327. Deve listar todas as ações disparadas pela plataforma de forma automática e manual;

13.1.328. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

13.1.329. Reagir programaticamente, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da CPTM;

13.1.330. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

13.1.331. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

13.1.332. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

13.1.333. Deve proteger o acesso a Aplicações Internas e na Nuvem.

13.1.334. A solução deve garantir que apenas usuários autenticados com dispositivos compatíveis possam se conectar a aplicativos autorizados e recursos de rede.

13.1.335. A solução deve suportar os seguintes sistemas IAM para gerenciar os usuários:

13.1.336. Azure AD

13.1.337. Okta

13.1.338. Active Directory

13.1.339. OpenLDAP

13.1.340. A solução deve ingerir dados do IAM conectado para analisar o comportamento do usuário e avaliar o risco.

13.1.341. A soluçãdeve suportar a Execução de Política no sistema IAM para executar tarefas como Desativar Usuário ou Forçar Redefinição de Senha.

13.1.342. A solução deve suportar SSO via SAML 2.0 para integrar a autenticação de usuário.

13.1.343. O mesmo agente deve ser capaz de fazer Varreduras de Vulnerabilidade para avaliar o risco dos dispositivos.

13.1.344. A plataforma deve permitir a criação de regras baseadas em risco da seguinte forma:

13.1.345. A plataforma deve permitir a criação de regras baseadas em risco de forma gráfica, usando fluxogramas.

13.1.346. Deve permitir definir condições baseadas em nível de risco.

13.1.347. Deve permitir definir condições em situações específicas (conta encontrada na dark web, por exemplo, comportamento de ransomware detectado).

13.1.348. Deve permitir especificar agendamentos.

13.1.349. Deve permitir aplicar regras granularmente com base em usuários, grupos ou dispositivos.

13.1.350. Deve permitir especificar ações para Controle de Acesso Privado.

13.1.351. Deve permitir especificar ações para Controle de Acesso à Internet.

13.1.352. Deve permitir executar ações no IAM (por exemplo, desativar contas de usuário).

13.1.353. Deve permitir executar ações no nível do dispositivo (por exemplo, isolar o endpoint).

13.1.354. Deve permitir especificar ações de revogação se o risco diminuir ou após um limite;

13.1.355. A plataforma deve incluir modelos predefinidos para diferentes casos de uso.

13.1.356. 3.2.4.10 A solução deve ser capaz de executar as seguintes ações:

13.1.357. Desativar Conta de Usuário;

13.1.358. Forçar Logout;

13.1.359. Forçar Redefinição de Senha;

13.1.360. Ativar Conta de Usuário;

13.1.361. Isolar Endpoint;

13.1.362. Restaurar Conexão;

13.1.363. Monitorar Tentativas de Login;

13.1.364. Monitorar Acesso de Aplicativo Interno;

13.1.365. Bloquear Acesso de Aplicativo Interno;

13.1.366. Desbloquear Acesso de Aplicativo Interno;

13.1.367. Permitir Acesso de Aplicativo Interno;

13.1.368. Bloquear Acesso de Aplicativo/URL na Nuvem;

13.1.369. Desbloquear Acesso de Aplicativo/URL na Nuvem;

13.1.370. Permitir Acesso de Aplicativo/URL na Nuvem.

13.1.371. A solução deve ser capaz de avaliar a postura do dispositivo com pelo menos as seguintes verificações:

13.1.372. O dispositivo está executando uma das versões especificadas do sistema operacional;

13.1.373. O certificado CA da empresa está presente no Trust Store;

13.1.374. O certificado do cliente é assinado pelo CA da empresa;

13.1.375. Um arquivo especificado está presente no dispositivo;

13.1.376. O firewall está ativado para a rede conectada;

13.1.377. A detecção de vulnerabilidades está ativada;

13.1.378. O software antivírus de um dos fornecedores especificados está instalado/rodando;

13.1.379. Uma solução EDR de um dos fornecedores especificados está em execução;

13.1.380. O dispositivo faz parte de um domínio;

13.1.381. O bloqueio de tela está ativado;

13.1.382. A criptografia de disco está ativada no dispositivo

13.1.383. A solução deve atuar com funcionalidade de acesso seguro baseado na metodologia de Zero Trust, a fim de controlar o acesso a aplicativos internos, data centers e ambientes IaaS, por meio de gateway seguro.

13.1.384. O gateway seguro deve estar disponível como um appliance virtual para VMware e disponível nas principais provedoras de nuvem: Azure, AWS e GCP.

13.1.385. Cada Appliance Virtual deve suportar pelo menos 15k conexões simultâneas;

13.1.386. Os usuários devem ser capazes de acessar os aplicativos internos configurados no gateway por meio de um agente;

13.1.387. O agente deve suportar o encaminhamento de qualquer tráfego usando TCP ou UDP, em qualquer porta;

13.1.388. Os usuários devem ser capazes de acessar os aplicativos internos configurados no gateway sem agente por meio de um portal de usuário da web;

13.1.389. O portal de usuário da web deve suportar HTTP/HTTPS/RDP e SSH no navegador;

13.1.390. A solução deve permitir a configuração de um domínio personalizado para o portal da web.

13.1.391. Os usuários devem ser desconectados automaticamente do agente para acesso privado após um período de inatividade.

13.1.392. A solução deve fornecer um Zero Trust Secure Web Gateway (ZT SWG) que garanta o acesso seguro a sites externos.

13.1.393. A solução deve controlar o tráfego da web por meio de um agente instalado.

13.1.394. A solução deve controlar o tráfego da web usando arquivos PAC, encadeamento de proxy ou encaminhamento de porta para dispositivos nos quais não é possível instalar um agente.

13.1.395. O provedor deve ter um PoP (Point of Presence) no Brasil.

13.1.396. A solução deve fornecer um Gateway de Acesso à Internet em Nuvem.

13.1.397. A solução deve suportar um Gateway de Acesso à Internet Local.

13.1.398. A solução deve aplicar regras com base na localização do usuário.

13.1.399. A solução deve suportar regras/políticas de inspeção HTTPS.

13.1.400. A solução deve permitir impor regras com base em horários.

13.1.401. A solução deve suportar ações granulares dentro de um aplicativo em nuvem (bloquear o upload de arquivos para o Teams devido a comportamentos arriscados).

13.1.402. O Gateway On Premise gerenciado pelo console em nuvem deve suportar outras funções, como:

13.1.403. Integração de Firewall (Fortinet, Cisco, Palo Alto, Checkpoint e outros) para impor ações de bloqueio em nível de rede.

13.1.404. Integração de IAM para AD local, para impor ações e ingestão de dados de usuário.

13.1.405. Scanners de Vulnerabilidade como Qualys, Nessus e Tenable para ingestão de dados de vulnerabilidade para um controle de política de dispositivo granular.

13.1.406. Suporte de syslog para enviar dados para coletores SIEM locais.

13.1.407. A solução deve permitir especificar o tipo de mídia, nome de arquivo ou verdadeiro tipo de arquivo dos arquivos que são permitidos ou bloqueados para acessar para fins de segurança, monitoramento ou desempenho.

13.1.408. A solução deve permitir configurar regras de proteção, como:

13.1.409. Análise de Reputação de URL;

13.1.410. Detecção de Botnet;

13.1.411. Aprendizado de Máquina em arquivos sendo baixados

13.1.412. Bloqueio de IoC (IP/URL/Domínio/SHA-1)

13.1.413. Análise de arquivos compactados de até 15 camadas de compactação

13.1.414. Verificação de arquivos de até 2 GB.

13.1.415. Regras de DLP para examinar o tráfego da web de saída em busca de conteúdo, incluindo dados confidenciais;

13.1.416. Deve permitir bloquear todas as Aplicações em Nuvem Não Autorizadas

13.1.417. Deve suportar Tenancy Restrictions para permitir que um usuário faça login em um aplicativo em nuvem apenas com suas contas corporativas, em vez de contas pessoais.

13.1.418. Deve ter Aplicativos em Nuvem suportados predefinidos

13.1.419. Deve permitir definir Aplicativos em Nuvem personalizados.

13.1.420. Deve permitir definir exceções de Inspeção HTTPS.

13.1.421. Deve permitir impor o uso do Modo Restrito no Google, Yahoo e Bing.

13.1.422. Gateway Web On Premise para redirecionar o tráfego.

13.1.423. Portal da Web para acessar aplicativos internos sem agente.

13.1.424. Deve elencar o nível de risco cibernético dos usuários da CPTM, identificando os que apresentem comportamentos anômalos de:

13.1.424.1. Comprometimento de credencial;

13.1.424.2. Ataque de força bruta;

13.1.424.3. Login atípico ou impossível;

13.1.424.4. Login via IPs suspeitos;

13.1.424.5. Múltiplas tentativas de login com sucesso e insucesso;

13.1.425. A partir da dos alertas de risco dos usuários, deve ser possível enviar ações de mitigação de risco:

13.1.425.1. Forçar reset de senha;

13.1.425.2. Desabilitar conta do usuário no serviço de diretório;

13.1.425.3. Forçar sign-out do usuário;

13.1.426. Deverá centralizar as ações e estender a visibilidade sob todas as funcionalidades, sendo elas:

13.1.426.1. Inspeção de rede contra ameaças avançadas com detecção e resposta;

13.1.426.2. Detecção e resposta para Servidores e cargas de trabalho;

13.1.426.3. Detecção e resposta para estações de trabalho;

13.1.426.4. Controle de acesso a aplicações internas, externas e na nuvem;

13.1.426.5. Prevenção de Intrusão de rede;

13.1.427. A solução deverá prover relatórios contendo no mínimo as seguintes informações:

13.1.427.1. Top Ameaças;

13.1.427.2. Top usuários com risco;

13.1.427.3. Top vulnerabilidades identificadas;

13.1.427.4. Top Hosts com detecções;

13.1.427.5. Sumário de tráfego de rede inspecionado;

SOLUÇÃO DE SEGURANÇA DE SERVIDORES DE SISTEMA

13.1.428. A solução deve prover proteção avançada com base em capacidades de proteção contra ameaças avançadas e de dia zero que almejem comprometer os servidores de sistema da CONTRATANTE;

13.1.429. Deve possuir módulo específico de prevenção de ataques via exploits e exploração de vulnerabilidades;

13.1.430. Deve possuir módulo de Anti-malware de próxima geração, proteção contra acessos Web, Firewall de host próprio da solução, controle de aplicações, monitor de integridade de arquivos, DLLs e logs do sistema operacional e IPS contra ameaças via exploração de rede;

13.1.431. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

13.1.432. A console de administração deverá permitir o envio de notificações via SMTP;

13.1.433. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

13.1.434. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

13.1.435. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

13.1.436. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

13.1.437. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

13.1.438. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

13.1.439. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

13.1.440. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

13.1.441. A solução de segurança ter a capacidade de identificar ataques em estruturas de container.

13.1.442. Deve ser possível customizar os privilégios de administração da solução:

13.1.442.1. Acesso total;

13.1.442.2. Acesso somente leitura;

13.1.443. Deve ser possível assignar políticas de segurança em máquinas específicas, grupos estáticos e dinâmicos;

13.1.444. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

13.1.445. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

13.1.446. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

13.1.447. 13.1.420. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

13.1.447.1. Windows Server 2003 SP1;

13.1.447.2. Windows Server 2003 R2 SP2;

13.1.447.3. Windows Server 2008;

13.1.447.4. Windows Server 2008 R2;

13.1.447.5. Windows Server 2012;

13.1.447.6. Windows Server 2012 R2;

13.1.447.7. Windows Server 2016;

13.1.447.8. Windows Server 2019;

13.1.447.9. Windows Server 2022;

13.1.447.10. Red Hat Enterprise 5, 6, 7 e 8;

13.1.447.11. CentOS 6, 7 e 8;

13.1.447.12. Oracle Linux 5, 6, 7 e 8;

13.1.447.13. SUSE Linux Enterprise Server 10, 11, 12 e 15;

13.1.447.14. Ubuntu 10, 12, 14, 16, 18 e 20;

13.1.447.15. Debian 6, 7, 8, 9 e 10;

13.1.447.16. Rocky Linux 8;

13.1.448. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

13.1.449. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

13.1.450. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

13.1.451. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

13.1.452. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

13.1.453. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

13.1.454. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

13.1.455. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

13.1.456. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

13.1.457. A solução deverá mostrar quais máquinas estão usando determinada política;

13.1.458. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

13.1.459. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

13.1.460. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

13.1.461. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

13.1.462. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

13.1.463. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

13.1.464. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

13.1.465. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

13.1.466. A solução deverá ter a capacidade de se integrar com soluções de SIEM;

13.1.467. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

13.1.468. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

13.1.469. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

13.1.470. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

13.1.471. Após a atualização deve ser informado o que foi modificado ou adicionado;

13.1.472. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

13.1.473. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

13.1.474. A solução deverá ter capacidade de gerar pacote de autodiagnostico de modo a coletar arquivos relevantes para envio ao suporte do produto;

13.1.475. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

13.1.476. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

13.1.477. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

13.1.478. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

13.1.479. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

13.1.480. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

13.1.481. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

13.1.482. A solução deve possuir API documentada para integração na esteira de automação;

13.1.483. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

13.1.484. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

13.1.485. A solução deve permitir desabilitar os módulos individualmente;

13.1.486. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

13.1.487. A console deverá possibilitar a integração com o Microsoft Active Directory, listando as máquinas e grupos existentes na estrutura;

13.1.488. Em caso de a solução ser ofertada em nuvem, deve ser compliance com ISO 27001, ISO 27014, ISO 27017 e SOC 2;

13.1.489. Os ambientes em nuvem providos pelo fabricante devem passar por testes de penetração de forma recorrente como para garantir a segurança da solução provida.

13.1.490. Deverá possuir funcionalidade de Antimalware;

13.1.491. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

13.1.492. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

13.1.493. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

13.1.494. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

13.1.495. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de

arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

13.1.496. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentena de arquivos identificados;

13.1.497. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

13.1.498. A solução deverá oferecer escanear processos em memória em busca de Malware;

13.1.499. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

13.1.500. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;

13.1.501. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

13.1.502. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

13.1.503. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

13.1.504. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

13.1.505. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

13.1.506. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

13.1.507. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

13.1.508. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

13.1.509. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

13.1.510. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

13.1.511. Proteção contra URLs Maliciosas

13.1.512. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

13.1.513. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

13.1.514. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

13.1.515. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

13.1.516. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

13.1.517. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

13.1.518. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

13.1.519. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

13.1.520. Deverá possuir funcionalidade de Firewall de host;

13.1.521. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

13.1.522. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

13.1.523. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

13.1.524. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

13.1.525. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

13.1.526. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

13.1.527. Precisa ter a capacidade de definição de regras para contextos específicos;

13.1.528. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

13.1.529. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

13.1.530. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

13.1.531. O firewall deverá ser stateful bidirecional;

13.1.532. O firewall deverá permitir liberar ou apenas logar eventos;

13.1.533. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

13.1.534. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

13.1.535. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

13.1.536. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

13.1.537. Deverá realizar pseudo stateful em tráfego UDP;

13.1.538. Deverá logar a atividade stateful;

13.1.539. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

13.1.540. Deverá permitir limitar o número de meias conexões vindas de um computador;

13.1.541. Deverá prevenir ack storm;

13.1.542. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

13.1.543. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;

13.1.544. Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;

13.1.545. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

13.1.546. Proteção contra Vulnerabilidades de Sistemas Operacionais e Aplicações

13.1.547. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

13.1.548. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do Sistema Operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

13.1.549. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

13.1.550. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

13.1.551. recisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

13.1.552. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

13.1.553. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

13.1.554. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

13.1.555. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

13.1.556. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

13.1.557. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

13.1.558. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

13.1.559. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

13.1.560. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

13.1.561. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

13.1.562. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

13.1.563. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

13.1.564. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

13.1.565. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

13.1.566. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

13.1.567. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

13.1.568. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

13.1.569. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

13.1.570. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

13.1.571. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

13.1.572. As regras devem ser atualizadas automaticamente pelo fabricante;

13.1.573. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

13.1.574. Monitoramento De Integridade para Servidores

13.1.575. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

13.1.576. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

13.1.577. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

13.1.578. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

13.1.579. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

13.1.580. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

13.1.581. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

13.1.582. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

13.1.583. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;

13.1.584. Deverá logar e colocar em relatório todas as modificações que ocorram;

13.1.585. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

13.1.586. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

13.1.587. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

13.1.588. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

13.1.589. Deverá possuir capacidade de Inspeção de Logs para Servidores

13.1.590. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft e AIX;

13.1.591. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

13.1.592. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de

inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

13.1.593. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

13.1.594. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

13.1.595. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

13.1.596. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

13.1.597. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

13.1.598. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

13.1.599. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

13.1.600. As regras poderão ser modificadas por severidade de ocorrência de eventos;

13.1.601. As regras devem se atualizar automaticamente pelo fabricante;

13.1.602. Permitir modificação pelo administrador em regras para adequação ao ambiente.

13.1.603. Deverá possuir capacidades de Controle De Aplicações

13.1.604. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

13.1.605. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

13.1.606. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

13.1.607. A console deverá exibir eventos de no mínimo 30 dias;

13.1.608. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

13.1.609. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

13.1.610. Deverá possuir funcionalidades de Detecção e Resposta;

13.1.611. solução deve possuir módulo de investigação, detecção integrados;

13.1.612. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

13.1.613. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

13.1.614. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

13.1.615. O módulo de detecção e resposta deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

13.1.616. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

13.1.617. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

13.1.618. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

13.1.619. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

13.1.620. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

13.1.621. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

13.1.622. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

13.1.623. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

13.1.624. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

13.1.625. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

13.1.626. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

13.1.627. 13.1.600. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

13.1.628. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de detecção e resposta do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;

13.1.629. Esta conexão deverá garantir, sem qualquer configuração local, que o sensor de detecção e resposta esteja ativo e envie telemetria a plataforma.

14. SERVIÇOS NO AMBIENTE DE TI DA CPTM

CPTM prima pela adoção das melhores práticas e alocação de profissionais qualificados no gerenciamento dos recursos de TI escopo desta contratação;

A CONTRATADA deverá seguir todas as diretrizes determinadas por normativos internos elaborados pela CPTM, bem como os procedimentos operacionais.

A CONTRATADA deverá ter ciência, observar e respeitar a Política de Governança de Dados e Informações (PGDI) e a Política de Proteção de Dados Pessoais (PPDP) do estado de São Paulo, instituída pelo decreto nº 65.347, de 9 de dezembro de 2020 e publicada no Diário Oficial do Estado em 31/12/2021, página 14 do caderno Executivo I (Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021 e Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021).

O objetivo é entregar e prestar o suporte aos serviços de TI garantindo que estejam em sintonia com os requerimentos de negócio da organização. O ITIL 4 oferece um conjunto de melhores práticas: completo, consistente e coerente, para o gerenciamento de serviços suportados por TI, promovendo uma abordagem de qualidade para atingir a eficácia e eficiência do negócio no uso dos sistemas de informação. Tais práticas devem ser implementadas de forma a amparar os processos de negócio da organização.

A CONTRATADA deve se utilizar, no mínimo, das seguintes práticas ITIL 4 para a realização do atendimento do escopo dessa contratação:

14.1. PRÁTICAS GERAIS DE GERENCIAMENTO ITIL 4

14.1.1. GERENCIAMENTO DE ESTRATÉGIA

Gerencia planos e ações para o cumprimento adequado dos objetivos de negócio, em conformidade com as diretrizes e prioridades definidas.

O objetivo da prática de gestão estratégica é formular os objetivos da organização e adotar diretrizes de ação e alocação de recursos necessários para atingir esses objetivos. A gestão estratégica estabelece a direção da organização, concentra esforços, define ou esclarece as prioridades da organização e fornece consistência ou orientação em resposta ao ambiente.

O ponto de partida para a gestão da estratégia é compreender o contexto da organização e definir os resultados desejados. A estratégia da organização estabelece critérios e mecanismos que ajudam a decidir a melhor forma de priorizar recursos, capacidades e investimentos para alcançar esses resultados, enquanto a prática garante que a estratégia seja definida, acordada, mantida e alcançada.

A CONTRATADA deve utilizar as práticas de gerenciamento de estratégia, incluindo, mas não se limitando, para:

14.1.1.1. Analisar o ambiente em que a companhia existe para identificar oportunidades que beneficiarão a CPTM;

14.1.1.2. Identificar restrições que possam impedir a obtenção de resultados e definir como essas restrições poderiam ser removidas ou seus efeitos reduzidos;

14.1.1.3. Garantir que a estratégia seja traduzida em planos táticos e operacionais e distribuída para cada serviço constante nesse Termo de Referência, visando cumprir a estratégia determinada pela CPTM;

14.1.1.4. Garantir que a estratégia seja implementada através da execução dos planos estratégicos e a coordenação de esforços, acompanhando mudanças nos ambientes internos e externos e outros fatores relevantes.

14.1.2. GERENCIAMENTO DE FORNECEDORES

Gerencia os provedores de serviço da organização, de forma que as entregas por eles realizadas mantenham os padrões definidos.

O objetivo da prática de gerenciamento de fornecedores é garantir que os fornecedores da organização e o seu desempenho sejam geridos de forma adequada para apoiar o fornecimento contínuo de produtos e serviços de qualidade. Isto inclui a criação de relações mais próximas e colaborativas com os principais fornecedores para descobrir e concretizar novo valor e reduzir o risco de fracasso.

14.1.2.1. A CONTRATADA deve utilizar as práticas de Gerenciamento de Fornecedores na gestão dos serviços.

14.1.2.2. A CONTRATADA deve criar um ponto único de visibilidade e controle para garantir consistência de todos os produtos, serviços, componentes de serviço e procedimentos fornecidos ou operados por fornecedores internos e externos.

14.1.2.3. A CONTRATADA deve medir o desempenho dos fornecedores, monitorando os termos, condições e metas dos contratos e acordos.

14.1.3. MEDIÇÃO E RELATÓRIOS

Disponibiliza informações importantes ao negócio para a tomada de decisões em diversos níveis da organização, referentes à cadeia completa de serviço.

O objetivo da prática de medição e relatórios é apoiar a boa tomada de decisões e a melhoria contínua, diminuindo os níveis de incerteza. Isto é conseguido através da coleta de dados relevantes sobre os vários objetos geridos e da validação destes dados num contexto apropriado. Os objetos gerenciados incluem, entre outros, produtos e serviços, práticas e atividades da cadeia de valor, equipes e indivíduos, fornecedores e parceiros, e a organização como um todo.

14.1.3.1. A CONTRATADA deve, de acordo com tal prática, realizar medições e emitir relatórios que permitirão decisões estratégicas e de portfólio de serviços, fornecendo detalhes sobre o desempenho atual de produtos e serviços.

14.1.3.2. A CONTRATADA deve monitorar e avaliar o desempenho constantemente para sustentar a ações de melhoria contínua, alinhamento e a criação de valor.

14.1.3.3. A CONTRATADA deve entregar relatórios que forneçam informações para decisões de gerenciamento.

14.1.4. GERENCIAMENTO DE PROJETOS

Gerencia as atividades relacionadas aos projetos da organização, de forma que sejam apropriadamente conduzidos e cumpram seus objetivos, dentro do escopo, prazo e custos estimados.

O objetivo da prática de gerenciamento de projetos é garantir que todos os projetos da organização sejam entregues com sucesso. Isto é conseguido planejando, delegando, monitorando e mantendo o controle de todos os aspectos de um projeto, e mantendo a motivação das pessoas envolvidas.

14.1.4.1. A CONTRATADA deve utilizar tal prática para controlar e entregar os objetivos dos projetos solicitados.

14.1.5. GESTÃO DO CONHECIMENTO

Gerencia uma base de conhecimento, contendo o histórico dos atendimentos e sua solução, a fim de que possa auxiliar na resolução de novos problemas e na tomada de decisões.

O objetivo da prática de gestão do conhecimento é manter e melhorar o uso eficaz, eficiente e conveniente da informação e do conhecimento em toda a organização.

O conhecimento é um dos ativos mais valiosos de uma organização. A prática de gestão do conhecimento fornece uma abordagem estruturada para definir, construir, reutilizar e compartilhar conhecimento (ou seja, informações, habilidades, práticas, soluções e problemas) em diversas formas. À medida que os métodos de captura e partilha de conhecimento avançam mais para soluções digitais, a prática da gestão do conhecimento torna-se ainda mais valiosa.

14.1.5.1. A CONTRATADA deve utilizar tal prática, visando garantir que as partes interessadas obtenham a informação certa, no formato adequado, ao nível certo e no momento correto, de acordo com o seu nível de acesso e políticas relevantes.

14.1.5.2. A CONTRATADA deve estabelecer procedimentos para a aquisição, tratamento, armazenamento e disponibilização do conhecimento de todo o ambiente de TI da CPTM, incluindo conhecimento não estruturado, efetivando o conhecimento informal e tácito em formal e documentado.

14.1.6. GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO

Gerencia todos os aspectos pertinentes à segurança da informação do negócio (por exemplo, dados confidenciais, acessos.).

O objetivo da prática de gerenciamento de segurança da informação é proteger as informações necessárias à organização para conduzir seus negócios. Isso inclui compreender e gerenciar riscos à confidencialidade, integridade e disponibilidade das informações, bem como os aspectos da segurança da informação, como autenticação (garantir que alguém é quem afirma ser) e não repúdio (garantir que alguém não possa negar que eles tomaram uma ação).

Observando tal prática, a CONTRATADA deve:

14.1.6.1. Propor e seguir processo gerenciamento de incidentes de segurança da informação estabelecidos pela CPTM;

14.1.6.2. Propor e seguir processo de gerenciamento de riscos e processo de revisão de controle e auditoria estabelecidos pela CPTM;

14.1.6.3. Propor e seguir um processo de gerenciamento de identidade e acesso estabelecidos pela CPTM;

14.1.6.4. Propor e seguir procedimentos para gerenciamento de eventos, para testes de penetração e verificação de vulnerabilidades estabelecidos pela CPTM;

14.1.6.5. Propor e seguir procedimentos para gerenciar alterações relacionadas à segurança da informação estabelecido pela CPTM.

14.1.7. GERENCIAMENTO DE RISCOS DO AMBIENTE DE TIC

Gerencia os riscos que possam impactar o andamento do negócio, identificando-os previamente e prevendo ações para o seu tratamento.

O objetivo da prática de gestão de riscos é garantir que a organização compreenda e lide eficazmente com os riscos. A gestão do risco é essencial para garantir a sustentabilidade contínua de uma organização e criar valor para os seus clientes. A gestão de riscos é parte integrante de todas as atividades organizacionais e, portanto, central para o Sistema de Valor de Serviços da organização.

Observando tal prática, a CONTRATADA deve:

14.1.7.1. Identificar, registrar e analisar incertezas que podem afetar o alcance dos objetivos no contexto de uma atividade específica. Estas incertezas devem ser consideradas e depois descritas para garantir que haja um entendimento comum;

14.1.7.2. Avaliar e estimar a probabilidade, o impacto e a proximidade dos riscos individuais;

14.1.7.3. Priorizar o nível geral de risco (exposição ao risco) associado à determinada atividade.

14.1.7.4. Responder adequadamente aos riscos realizando planejamentos, atribuindo proprietários e intervenientes. Após a implementação dos planos, monitorar e controlar os resultados.3

14.2. PRÁTICAS DE GERENCIAMENTO DE SERVIÇOS ITIL 4

14.2.1. GERENCIAMENTO DE ATIVOS DE TI

Gerencia os bens e os componentes relacionados com o serviço de TI, mantendo o controle sobre seu ciclo de vida, a fim de que continuem agregando valor para a organização.

O objetivo da prática de gerenciamento de ativos de TI é planejar e gerenciar o ciclo de vida completo de todos os ativos de TI, para ajudar

a organização, dentre outras coisas, a maximizar seu valor, controlar custos, gerenciar riscos, apoiar a tomada de decisões sobre compra, reutilização, retirada e alienação de ativos e atender aos requisitos regulatórios e contratuais. A gestão de ativos de TI contribui para a visibilidade dos ativos e do seu valor, o que é um elemento-chave para uma gestão de serviços bem-sucedida, além de ser útil para outras práticas.

Observando tal prática, a CONTRATADA deve:

14.2.1.1.1. Identificar os ativos físicos com etiquetas e códigos específicos para cada tipo de ativo. A CONTRATADA deverá providenciar e disponibilizar etiquetas de identificação dos Ativos de TI da CPTM, para facilitar a realização e controle do inventário de hardware. As etiquetas deverão seguir o padrão já existente na CPTM;

14.2.1.1.2. Fornecer etiquetas autoadesivas para identificação dos ativos de TIC de responsabilidade da CONTRATADA, com dimensões de 2 cm x 3 cm, resistentes, de fácil leitura e durabilidade compatível com o ambiente operacional, mantendo o padrão visual atualmente adotado pela CONTRATANTE, inclusive quanto a layout, tipografia e codificação utilizada.

14.2.1.1.3. Realizar e manter atualizado o inventário dos Ativos de TI que sustentam os serviços da CPTM, mantendo dados históricos;

14.2.1.1.4. Identificar e controlar as licenças de software dos equipamentos de TI tais como: softwares e firmwares dos ativos de rede, dos servidores, dos roteadores, dos switches; licenciamento de portas de switches; chaves de licença do hypervisor;

14.2.1.1.5. Controlar a localização física de todos os ativos de hardware e softwares do ambiente de TI da CPTM, tais como: softwares armazenados em mídia física, chaves de registro de softwares em meio físicos servidores, storages, appliances e elementos de rede como firewalls,

roteadores, switches, access points ou qualquer outro ativo de TI;

14.2.1.1.6. Gerenciar o parque de tecnologia, acompanhando todo o ciclo de vida dos Ativos de TI (planejamento, execução, implantação, monitoramento, manutenção e descarte), conforme escopo definido no item 1 – DESCRIÇÃO DO AMBIENTE DE TI, incluindo, quando aplicável, roteadores, switches, servidores, estações de trabalho, periféricos, ativos de rede e links de comunicação contemplados para atendimento pelas equipes de Outsourcing;

14.2.1.1.7. Dentre as atividades listadas, a manutenção e o suporte dos equipamentos e demais soluções deverão ser realizados por meio de contratos de suporte firmados pela CONTRATANTE junto a seus fornecedores, ou por representantes autorizados;

14.2.1.1.8. Na ausência de serviços de suporte e manutenção ativos para determinados equipamentos, caso seja necessária a execução de atualização de firmware, a CONTRATADA deverá elaborar e apresentar previamente à CONTRATANTE um relatório técnico contendo a análise de riscos da atividade, solicitando sua aprovação formal e anuência expressa quanto aos riscos apontados. A execução da atividade somente deverá ocorrer após a autorização da CONTRATANTE, não cabendo à CONTRATADA qualquer responsabilidade ou ônus por eventuais falhas ou indisponibilidades decorrentes dessa atualização.

14.2.1.1.9. Utilizar o gerenciamento de Ativos de TI integrado com as demais práticas, como gerenciamento de configuração de serviço, gerenciamento de incidentes, habilitação de mudanças.

14.2.1.1.10. Garantir que os termos de licença sejam respeitados e que as licenças sejam reutilizadas apenas

de maneiras permitidas pelo contrato do software em questão.

14.2.1.1.11. Auditar ativos, mídia relacionada e conformidade (particularmente com regulamentações e termos e condições de licença) e conduzir melhorias corretivas e preventivas para lidar com problemas detectados.

14.2.1.1.12. Identificar e controlar ativos baseados em nuvem relacionando com os tipos de serviços, gerenciando os custos.

14.2.1.1.13. Realizar o teste e a emissão de parecer a respeito de qualquer novo ativo adotado pela CPTM, para os fins de homologação, devendo emitir nota técnica a respeito do impacto deste novo ativo no ambiente de produção da CPTM. Com base na nota técnica elaborada, a CPTM irá deliberar sobre a liberação de tal ativo no ambiente. Se o processo de liberação do ativo implicar em riscos de paralisação de quaisquer serviços considerados prioritários, deverá ser tratado como um projeto, sem ônus adicional a CPTM e com acordo de nível de serviço (SLA) negociado entre ambas as partes, caso a caso;

14.2.2. GERENCIAMENTO DE CONFIGURAÇÃO DE SERVIÇO

Gerencia os itens de configuração associados aos serviços da organização, a fim de realizar um melhor controle sobre cada um deles.

O objetivo da prática de gerenciamento de configuração de serviços é garantir que informações precisas e confiáveis sobre a configuração dos serviços e os ICs (Item de Configuração - Qualquer componente que precise ser gerenciado para fornecer um serviço de TI), que os suportam, estejam disponíveis quando e onde forem necessárias. Isso inclui informações sobre como os ICs são configurados e os relacionamentos entre eles.

O gerenciamento de configuração de serviço coleta e gerencia informações sobre uma ampla variedade de ICs, incluindo hardware, software, redes, edifícios, pessoas, fornecedores e documentação. Os serviços também são tratados como ICs, e o gerenciamento de configuração ajuda a organização a compreender como os vários ICs, que contribuem para cada serviço, funcionam juntos. Já o Sistema de Gerenciamento de Configuração (CMS) é um conjunto de ferramentas, dados e informações que são usados para dar suporte ao gerenciamento de configuração de serviço.

Observando tal prática, a CONTRATADA deve:

14.2.2.1. Manter atualizado o CMS existente na CPTM, conforme ICs definidos em conjunto entre a CPTM e a CONTRATADA, decorrente da necessidade de controle dos mesmos, porém, com decisão final da CPTM;

14.2.2.2. Identificar ICs, seus relacionamentos e adicioná-los ao sistema de gerenciamento de configuração (CMS CPTM). Tais informações serão essenciais para compor registros de incidentes, problemas e mudanças com a qualidade esperada;

14.2.2.3. Manter controle de versão, estabelecer linhas de base e realizar monitoramento dos ICs.

14.2.2.4. Atualizar dados dos Itens de Configuração (ICs) quando as alterações forem implantadas, decorrentes ou não da prática de Habilitação de Mudança;

14.2.2.5. Validar veracidade dos registros de configuração;

14.2.2.6. Auditar aplicativos e infraestrutura para identificar a ausência de documentação.

14.2.3. GERENCIAMENTO DE CATÁLOGO DE SERVIÇOS

Gerencia a listagem de produtos e serviços ofertados pela organização aos seus clientes.

O objetivo da prática de gerenciamento de catálogo de serviços é fornecer uma fonte única de informações consistentes sobre todos os serviços e ofertas de serviços e garantir que estejam disponíveis para o público relevante.

Observando tal prática, a CONTRATADA deve:

14.2.3.1. A CONTRATADA deverá elaborar o catálogo de serviços, com a descrição dos serviços de TI que serão prestados aos usuários de TI da CPTM. O levantamento, organização e sua disponibilização não deverão ultrapassar 90 dias corridos da emissão da Ordem de Serviço e deverá ser aprovado pela CPTM.

14.2.3.2. Publicar, editar e manter descrições de serviços e produtos e suas ofertas relacionadas. Fornecer visão sobre o escopo de quais serviços estão disponíveis e em que termos. O catálogo deverá descrever as características dos serviços através das funcionalidades e garantias providas e quais grupos de usuários são clientes de cada serviço de TI.

14.2.3.3. Gerenciar, editar e manter atualizada a lista de serviços disponíveis à medida que forem introduzidos, alterados ou desativados.

14.2.4. GERENCIAMENTO DE DISPONIBILIDADE

Garante que os serviços atendam às necessidades atuais e futuras de disponibilidade do negócio, de maneira oportuna e eficaz em custo.

O objetivo da prática de gerenciamento de disponibilidade é garantir que os serviços forneçam níveis acordados de disponibilidade para atender às necessidades dos clientes e usuários.

Observando tal prática, a CONTRATADA deve:

14.2.4.1. Negociar e concordar com metas atingíveis para disponibilidade

14.2.4.2. Projetar infraestrutura e aplicativos que possam fornecer os níveis de disponibilidade necessários

14.2.4.1. Garantir que serviços e componentes sejam capazes de coletar os dados necessários para medir a disponibilidade

14.2.4.2. Monitorar, analisar e relatar a disponibilidade

14.2.4.3. Planejar melhorias na disponibilidade

14.2.5. MONITORAMENTO E GERENCIAMENTO DE EVENTOS

Realiza o controle dos eventos que ocorrem na organização, prevendo possíveis impactos e atuando com proatividade em suas respostas.

O objetivo da prática de monitoramento e gerenciamento de eventos é observar sistematicamente os serviços e componentes de serviços e registrar e relatar alterações de estado selecionadas identificadas como eventos. Esta prática identifica e prioriza infraestrutura, serviços, processos de negócios e eventos de segurança da informação. Estabelece também a resposta apropriada a esses eventos, incluindo a resposta a condições que possam levar a possíveis falhas ou incidentes.

Evento: Qualquer mudança de estado que tenha significado para o gerenciamento de um serviço ou outro item de configuração (IC). Os eventos normalmente são reconhecidos por meio de notificações criadas por um serviço de TI, IC ou ferramenta de monitoramento.

Observando tal prática, a CONTRATADA deve:

14.2.5.1. Identificar quais serviços, sistemas, ICs ou outros componentes de serviço devem ser monitorados e estabelecer a estratégia de monitoramento visando garantir a disponibilidade e a qualidade do serviço;

14.2.5.2. Implementar e manter o monitoramento, aproveitando tanto os recursos nativos dos elementos observados quanto o uso de ferramentas de monitoramento específicas;

14.2.5.3. Monitorar, por meio de observação sistemática, ICs que sustentam os serviços para detectar condições de

significância potencial. Sempre que possível, deverá ser realizado de forma altamente automatizada.

14.2.5.4. Monitorar e gerenciar os eventos visando minimizar ou eliminar impactos negativos nos serviços;

14.2.5.5. Registrar e gerenciar essas mudanças de estado monitoradas que são definidas pela CPTM como um evento, determinando sua significância e identificando e iniciando a ação de controle correta para gerenciá-las.

14.2.5.6. Estabelecer e manter os limites e critérios para determinar quais mudanças de estado serão tratadas como eventos e elencar critérios para definir cada tipo de evento (informativo, aviso ou exceção);

14.2.5.7. Estabelecer e manter processos sobre como cada tipo de evento detectado deve ser tratado para garantir o gerenciamento adequado;

14.2.5.8. Implementar processos e automações necessários para operacionalizar os limites, critérios e políticas definidos.

14.2.6. GERENCIAMENTO DE CAPACIDADE E DESEMPENHO

Garante o atendimento das necessidades de capacidade e desempenho atuais e futuras do negócio, de maneira oportuna e eficaz em custo.

O objetivo da prática de gerenciamento de capacidade e desempenho é garantir que os serviços alcancem o desempenho acordado e esperado, satisfazendo a procura atual e futura de uma forma rentável.

A prática de gerenciamento de capacidade e desempenho geralmente lida com o desempenho do serviço e o desempenho dos recursos de suporte dos quais ele depende, como infraestrutura, aplicativos e serviços de terceiros.

Observando tal prática, a CONTRATADA deve:

14.2.6.1. Analisar e monitorar o desempenho atual do serviço;

14.2.6.2. Realizar modelagem de capacidade e desempenho, levando em consideração que serviços e componentes estejam dentro da capacidade e desempenho suportados e que recursos ociosos ou subutilizados sejam redimensionados de acordo com sua necessidade, a fim de evitar custos desnecessários.

14.2.6.3. Planejar melhorias e atendimento aos requisitos futuros possíveis realizando análise de requisitos de capacidade, prevendo alterações de demanda e otimização de desempenho;

14.2.6.4. Elaborar plano de capacidade e desempenho, garantindo que os recursos de TI sejam dimensionados adequadamente para atender às demandas atuais e futuras, proporcionando um desempenho satisfatório dos serviços de TI;

14.2.6.5. A CONTRATADA deve prover o monitoramento dos ativos da rede de dados e servidores da CPTM, quanto à carga e recursos disponíveis, comunicando com antecedência mínima de 180 dias corridos, qual a data provável de se esgotar 80% da capacidade dos recursos, baseado em projeção, através do monitoramento e planejamento da capacidade.

14.2.7. GERENCIAMENTO DE REQUISIÇÃO DE SERVIÇO

Realiza o controle e o atendimento das solicitações de serviços efetuadas pelos usuários, a fim de que estejam adequadas às suas necessidades.

O objetivo da prática de Gerenciamento de Requisição de Serviço é apoiar a qualidade acordada de um serviço, tratando todas as solicitações de serviço predefinidas e iniciadas pelo usuário de maneira eficaz e fácil de usar.

Uma requisição de serviço pode servir para uma ação de entrega de serviço (por exemplo, fornecer um relatório ou substituir um cartucho de

toner), uma solicitação de informações (por exemplo, como criar um documento ou qual é o horário de funcionamento do escritório), uma solicitação para fornecimento de um recurso ou serviço (por exemplo, fornecer um telefone ou laptop para um usuário ou fornecer um servidor virtual para uma equipe de desenvolvimento), uma solicitação para acesso a um recurso ou serviço (por exemplo, fornecer acesso a um arquivo ou pasta) ou mesmo para feedback, elogios e reclamações (por exemplo, reclamações sobre uma nova interface ou elogios a uma equipe de suporte).

Observando tal prática, a CONTRATADA deve:

14.2.7.1. Registrar toda requisição de serviço em ferramenta ITSM disponibilizada pela CPTM;

14.2.7.2. Automatizar, no maior nível possível, as requisições de serviço e seus procedimentos para atendimento;

14.2.7.3. Seguir as diretrizes sobre quais requisições serão atendidas com ou sem nenhum tipo de aprovação, de acordo com as definições da CPTM;

14.2.7.4. Propor prazos de atendimento, levando em consideração as expectativas dos usuários quanto aos tempos de atendimento, baseados no que a CPTM e a CONTRATADA podem, realisticamente, entregar;

14.2.7.5. Elaborar e seguir fluxos de trabalho para documentar e redirecionar qualquer solicitação, reclassificando corretamente as solicitações dos usuários, quando necessário.

14.2.7.6. Elaborar e propor processos e procedimentos bem desenhados, preferencialmente operacionalizados por meio de ferramentas de rastreamento e automação, visando maximizar a eficiência dos atendimentos às requisições. Efetivar tais propostas, após aprovação da CPTM;

14.2.8. GERENCIAMENTO DE INCIDENTES:

Restabelece o funcionamento normal do serviço após a ocorrência de um evento negativo, para que os impactos causados sejam os mínimos possíveis.

O objetivo da prática de gerenciamento de incidentes é minimizar o impacto negativo dos incidentes, restaurando a operação normal do serviço o mais rápido possível.

Cada incidente deve ser registrado e gerenciado para garantir que seja resolvido em um tempo que atenda às expectativas do cliente e usuário. Os tempos de resolução alvo são acordados, documentados e comunicados para garantir que as expectativas sejam realistas.

Observando tal prática, a CONTRATADA deve:

14.2.8.1. Categorizar, priorizar e registrar todo incidente em ferramenta ITSM disponibilizada pela CPTM;

14.2.8.2. Elaborar e propor classificação para garantir que os incidentes com maior impacto nos negócios sejam resolvidos primeiro. Efetivar tais propostas, após aprovação da CPTM;

14.2.8.3. Realizar gestão de incidentes com a adequada alocação de recursos para os diferentes tipos de incidentes.

14.2.8.4. Realizar o processo de investigação e diagnóstico, seguido da resolução e/ou recuperação, registrando as atividades na ferramenta ITSM disponível, mantendo informação de qualidade e em tempo adequado.

14.2.8.5. Utilizar e atualizar a base de conhecimento;

14.2.8.6. Envolver as áreas competentes e interessadas para que a colaboração de todos, com o compartilhamento de informações, ajude a resolver o incidente de forma mais eficiente e eficaz.

14.2.8.7. Em caso de alteração de ICs, realizar as atualizações necessárias (CMS e/ou inventário);

14.2.8.8. Realizar ou participar do processo de encerramento do incidente, validando se a ocorrência foi solucionada.

14.2.9. GERENCIAMENTO DE PROBLEMAS

Gerencia incidentes que ocorrem com frequência, cujo mapeamento já ocorreu após histórico do passado, buscando minimizar seus impactos nos serviços.

O objetivo da prática de gerenciamento de problemas é reduzir a probabilidade e o impacto dos incidentes, identificando as causas reais e potenciais dos incidentes e gerenciando soluções alternativas e erros conhecidos.

Os problemas estão relacionados a incidentes, mas devem ser diferenciados, pois são gerenciados de diferentes maneiras.

Os problemas são as causas, ou potenciais causas, de um ou mais incidentes. Requerem investigação e análise para identificar as causas, desenvolver soluções alternativas e recomendar uma resolução a longo prazo. Isso reduz o número e o impacto de incidentes futuros.

Observando tal prática, a CONTRATADA deve:

14.2.9.1. Adotar técnicas de gerenciamento de riscos para o gerenciamento de problemas (identificar, avaliar e controlar riscos);

14.2.9.2. Identificar problemas por meio de análise de tendências de registros de incidentes, de incidentes recorrentes, por informações recebidas de fornecedores e parceiros ou por informações recebidas de desenvolvedores de software internos;

14.2.9.3. Registrar os problemas identificados na ferramenta de ITSM da CPTM;

14.2.9.4. Analisar e priorizar problemas com maior potencial e probabilidade de impacto;

14.2.9.5. Realizar atividade de controle de erros;

14.2.9.6. A partir do controle de erros, requisitar as mudanças necessárias (prática de habilitação de mudança) para possíveis soluções;

14.2.9.7. A partir do controle de erros, verificar e avaliar a eficácia de possíveis soluções de contorno, buscando melhorias na solução;

14.2.9.8. Participar da revisão pós-implementação de soluções;

14.2.9.9. Realizar a análise do problema e a documentação de soluções de contorno e de erros conhecidos.

14.2.9.10. Verificar se, após execução da solução de um problema, o erro realmente foi corrigido.

14.2.10. HABILITAÇÃO DE MUDANÇA

Realizar o controle de mudanças relacionadas aos produtos e serviços ofertados pela organização. Esta prática é diferente do Gerenciamento de Mudanças Organizacionais (mais focada nas mudanças da estrutura da organização), situada nas Práticas Gerais de Gerenciamento.

O objetivo da prática de Habilitação de Mudança é maximizar o número de mudanças bem-sucedidas sem serviços e produtos, garantindo que os riscos foram avaliados adequadamente, autorizando a continuação das mudanças e gerenciando o cronograma de mudanças.

O escopo do controle de mudanças é definido por cada organização. Normalmente incluirá toda a infraestrutura de TI, aplicativos, documentação, processos, relacionamentos com fornecedores e qualquer outra coisa que possa impactar direta ou indiretamente um produto ou serviço.

Observando tal prática, a CONTRATADA deve:

14.2.10.1. A CPTM definirá os níveis de mudança que serão formalmente controlados e aqueles que terão um processo simplificado de gerenciamento, sendo estes os mais simples e com menor impacto no ambiente de TI;

14.2.10.2. A CPTM definirá os tipos de mudanças no ambiente, sendo que estas serão tratadas de forma diferenciada dos projetos;

14.2.10.3. A CPTM deverá classificar as mudanças por tipo (padrão, normal e emergencial) e atribuir a cada tipo seus respectivos requisitos;

14.2.10.4. A CPTM manterá um Comitê de Mudanças e a CONTRATADA deverá receber as solicitações de mudanças, preparar a reunião e participar das mesmas para prestar informações sobre os ambientes e serviços por ela executados. Mudanças que impliquem em um conjunto de procedimentos complexos, os quais envolvam várias equipes ou empresas CONTRATADAS e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverá ser tratado como um projeto, sem ônus adicional a CPTM e com acordo de nível de serviço (Service Level Agreement - SLA) negociado entre ambas as partes, caso a caso;

14.2.10.5. A CONTRATADA deverá apresentar ao Comitê de Mudanças da CPTM a proposta de todas as mudanças no ambiente de TI, conforme níveis de controle que serão estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto de sua realização;

14.2.10.6. A CONTRATADA deverá executar as mudanças no melhor horário para as atividades da CPTM, ocorrendo em quase sua totalidade fora do horário de expediente administrativo (8:00hs às 18:00hs), conforme acertado em reuniões de GMUD, sem ônus adicional a CPTM;

14.2.11. GERENCIAMENTO DE LIBERAÇÃO

Gerencia as versões entregues dos serviços ofertados, visando o seu atendimento aos requisitos e a satisfação dos seus usuários.

O objetivo da prática de gerenciamento de liberação é disponibilizar serviços e recursos novos e alterados para uso.

Observando tal prática, a CONTRATADA deve:

14.2.11.1. Elaborar métodos e procedimentos padronizados para planejar, agendar e controlar a construção, teste e implantação de liberações, para entregar novas funcionalidades requeridas pelo negócio, protegendo a integridade dos serviços existentes.

14.2.11.2. Implantar liberação no ambiente de produção de maneira controlada e planejada, para garantir a qualidade das implantações e a entrega de valor dos serviços de TI esperada pelo negócio.

14.2.11.3. Elaborar e propor um plano de liberação contendo, no mínimo, o escopo e conteúdo da liberação, a avaliação e perfil de risco, as partes interessadas e as áreas afetadas, a(s) equipe(s) responsável(eis) pela liberação, a agenda de implantação, a estratégia da liberação e implantação, os recursos necessários para a liberação, os ICs associados/impactados e o plano de retorno.

14.2.11.4. Seguir com o plano aprovado pela CPTM.

14.2.11.5. Verificar liberações que implicam em inclusão, alteração ou remoção de serviços e ICs para subsidiar o gerenciamento do catálogo de serviços, gerenciamento de configuração de serviço e o gerenciamento de ativos de TI.

14.2.12. GERENCIAMENTO DE CONTINUIDADE DE SERVIÇO

Realiza o planejamento para a recuperação de processos de negócio, caso ocorra uma interrupção dos serviços, visando reduzir os riscos a um nível aceitável.

O objetivo da prática de gestão de continuidade de serviço é garantir que a disponibilidade e o desempenho de um serviço sejam mantidos em níveis suficientes em caso de desastre. A prática fornece uma estrutura para construir resiliência organizacional com a capacidade de produzir uma resposta eficaz que salvaguarde os interesses das principais partes

interessadas e a reputação, a marca e as atividades de criação de valor da organização.

É acionado quando ocorre uma interrupção de serviço ou risco organizacional em uma escala maior do que a capacidade da organização de lidar com isso com práticas normais de resposta e recuperação, como gerenciamento de incidentes. Um evento organizacional desta magnitude é normalmente referido como um desastre. O gerenciamento de continuidade de serviço concentra-se nos eventos que a empresa considera significativos o suficiente para serem tratados como um desastre.

Observando tal prática, a CONTRATADA deve:

14.2.12.1. Elaborar conjunto de planos claramente definidos para recuperação de desastres, visando retornar o ambiente de TI a uma condição pré-desastre dentro dos prazos de negócios exigidos e acordados.

14.2.13. GERENCIAMENTO DE NÍVEL DE SERVIÇO

É responsável pela negociação dos acordos de níveis de serviço (service level agreement – SLA), garantindo que as práticas sejam adequadas para as metas de nível de serviço propostas.

O objetivo da prática de gestão de nível de serviço é definir metas claras baseadas no negócio para os níveis de serviço e garantir que a prestação de serviços seja adequadamente avaliada, monitorada e gerenciada em relação a essas metas.

Observando tal prática, a CONTRATADA deve:

14.2.13.1. Estabelecer uma visão compartilhada dos serviços e níveis de serviço almejados pelos usuários;

14.2.13.2. Realizar coleta, análise, armazenamento e emitir relatórios das métricas relevantes para os serviços;

14.2.13.3. Realizar revisões de serviço para garantir que o conjunto atual de serviços continue a atender às necessidades da CPTM e dos usuários;

14.2.13.4. Identificar e relatar problemas de serviço, incluindo desempenho em relação aos níveis de serviço definidos;

14.2.13.5. Propor, documentar, acordar, monitorar, medir, reportar e revisar o nível de serviço estabelecido;

14.2.13.6. Assegurar que metas específicas, mensuráveis e realísticas sejam desenvolvidas e que os usuários tenham uma expectativa clara e sem equívocos do nível de serviço a ser entregue;

14.2.13.7. Assegurar que medidas proativas para melhoria dos serviços sejam implementadas a custo justificável;

14.2.13.8. Monitorar e melhorar a satisfação do cliente com a qualidade do serviço entregue.

14.3. PRÁTICAS DE GERENCIAMENTO TÉCNICO ITIL 4

14.3.1. GERENCIAMENTO DE INFRAESTRUTURA E PLATAFORMA

Gerencia os recursos de infraestrutura do ambiente propriamente ditos, contemplando os produtos e serviços que estão em operação atualmente.

O objetivo da prática de gerenciamento de infraestrutura e plataforma é supervisionar a infraestrutura e as plataformas utilizadas por uma organização. Quando realizada de forma adequada, essa prática permite o monitoramento das soluções tecnológicas disponíveis para a organização, incluindo a tecnologia de prestadores de serviços externos.

Observando tal prática, a CONTRATADA deve:

14.3.1.1. Realizar a administração e gestão do Data Center e das salas técnicas que integram o ambiente de TI da CPTM, incluindo o monitoramento dos sistemas de energia, refrigeração, UPS, grupo motogerador, segurança física, CFTV, detecção e combate a incêndio, bem como das condições do piso falso nos ambientes de TI. O monitoramento deverá ser realizado por meio das

ferramentas, soluções e sistemas disponibilizados pela equipe ou empresa responsável pelo suporte e manutenção do Data Center, contratada diretamente pela CONTRATANTE ou por uma de suas demais contratadas.

14.3.1.2. Elaborar, propor e manter, em estado atualizado, as políticas, normas e procedimentos relacionado ao ambiente. Efetivar tais propostas, após aprovação da CPTM;

Manter minimamente:

14.3.1.1. Planos para proteção dos ambientes, definindo diretrizes de segurança de acesso, segurança da informação, manutenção e atualização dos processos, execução dos procedimentos, controles, auditorias, como por exemplo, que definam como a CPTM deseja que o datacenter seja administrado e mantido. A CONTRATADA, após a elaboração dos planos, baseando-se nas melhores práticas vigentes, apresentará a CPTM para apreciação e aprovação da mesma;

14.3.1.2. Procedimentos para definir os processos, que são as rotinas de manutenção e suporte que envolvem todas as áreas do datacenter ou salas técnicas, incluindo, mas não se limitando, os componentes a seguir:

14.3.1.2.1. Infraestrutura: Monitoramento de sistemas de: energia, refrigeração; UPS, grupo motogerador, segurança física, CFTV, detecção e combate a incêndio, piso falso;

14.3.1.2.2. Controles de segurança da informação, controles de acesso definindo quem e em qual situação o datacenter pode ser acessado;

14.3.1.2.3. Monitoramento dos riscos de ambiente, pessoal e de tecnologia;

14.3.1.2.4. Backup e recovery;

14.3.1.2.5. Gestão e manutenção da estrutura de cabling;

14.3.1.2.6. Gestão e gerenciamento dos ativos alocados no datacenter;

14.3.1.2.7. Controle e acompanhamento das manutenções preventivas, preditivas e corretivas;

14.3.1.2.8. Controle de acesso de terceiros.

15. ACORDO DE NÍVEL DE SERVIÇO – SLA

15.1. PERIODICIDADE DE AFERIÇÃO E AVALIAÇÃO

15.1.1. O período de aferição dos SLA's é mensal;

15.1.2. Deverão ser gerados automaticamente através de sistema(s) que coletam os dados diariamente e apontam o resultado do período (mensal);

15.1.3. Deverão constar de relatório todos os indicadores e metas de níveis de serviços contratados, além da descrição de chamados do período e recomendações técnicas, administrativas e gerenciais para o próximo período;

15.1.4. Periodicamente será realizada, entre a CPTM e a CONTRATADA, reunião de acompanhamento para verificação dos relatórios apresentados, análise dos resultados e dos planos de ação para correção de eventuais desvios;

15.1.5. Os primeiros 60 (sessenta) dias corridos após o início da execução dos serviços (emissão da OS) serão considerados como período de estabilização e de ajustes necessários, durante o qual os níveis de serviços estabelecidos serão aplicados, mas não será motivo de penalização contratual.

15.2. CRITICIDADE E NÍVEIS DE SERVIÇOS

15.2.1. Criticidade dos Incidentes

15.2.2. Criticidade Alta:

15.2.2.1. Incidentes que causam impacto em atividade crítica da CPTM, diretamente relacionados com a infraestrutura que suporta as aplicações de alta criticidade;

15.2.3. Criticidade Média:

15.2.3.1. Incidentes que causam impactos em atividades não críticas da CPTM, diretamente relacionados com a infraestrutura que suporta as aplicações de média criticidade;

15.2.4. Criticidade Baixa:

15.2.4.1. Incidentes que não causam impactos em atividades importantes, diretamente relacionados com a infraestrutura de aplicações de baixa criticidade;

15.3. CLASSIFICAÇÃO DE CRITICIDADE DOS SERVIÇOS

A CPTM possui aplicativos, os quais poderão ter acréscimo ao longo da execução do contrato, reclassificação quanto à criticidade, bem como a possibilidade de extinção e/ou sua substituição. Qualquer alteração na lista de aplicativos será efetivada após a negociação com a CONTRATADA.

15.3.1. SERVIÇOS DE ALTA CRITICIDADE:

Autenticação AD (Active Directory) - API
Alvo
Alvo - Faturamento - Vendas
App CPTM Web API
Serviço do App CPTM Oficial
Cadastro de Informações para exibição no Aplicativo CPTM
ASA - Acompanhamento de SA Simples
Controle de Validação de Bilhete de Serviço
CAP - Controle de Arrecadação de Passageiro
CAP - Controle de Arrecadação e Passageiro
Controle de Acesso a Sistemas
CIMG_CCO - Captura de Imagens Painéis Sinóticos CCO
CIMG_CCO.Captura.Service
CIMG_CCO - Coleta Service
CIMG_CCO - Localização
Compartilhado
Bilhetagem - Comunicacao SBE
BLT Comunicacao VBS
CRG - Controle de Circulação de Trens de Carga
CRG - Controle de Circulação de Trens de Carga (internet)
CVP - Controle de Vigilância e Portaria

CPTM.CVP.SERVICE
Ferramenta de Apoio Desenvolvimento Web
FDW.Service
Gestão de Atendimento
Gestão de Atendimento - Achados e Perdidos
CPTM.GAUAP.Service
CPTM.GAU.Service
Documentos Técnicos - consulta Intranet
Sistema de Controle da Frota, Localização do Material Rodante na Manutenção e Recolhimento de Trens
MIX
Sincronismo MIX x AD
Sincronismo MIX x AD
MIX - Avaliação e Pesquisas
MIX - Folha de Pagamento
MIX - Ponto Eletrônico
MixWeb - Avaliação e Pesquisas
MixWeb - Folha de Pagamento
MixWeb - Gestão de Escalas
MixWeb - PCCS
MixWeb - Ponto Eletrônico
MixWeb - Sobreaviso
MixWeb - Solicitação de Desligamento
Gestão de Redução de Bloqueios
Logística da Circulação
LOGÍSTICA DE ESTAÇÕES
Logística da Tração
Sistema Normativo
SGL - Sistema de Gestão de Limpeza
Gestão de Limpeza (internet)
Sharepoint - Intranet
Serviço do Portal CPTM - Central de Relacionamento
RDE - Relatório Diário de Estação
Regularidade
RETREM - Sistema de Recolhimento de Trens
Sistema de Recolhimento de Trens - RETREM_NET
Registro de Ocorrências de Pessoas
Administração Sistema de Segurança
SICOM - Sistema Integrado de Controle da Operação e Manutenção
Diário do CIM - Sistema de Informação da Manutenção
Alvo - Fiscal
Alvo - Estoque
Alvo - Materiais
Alvo - Financeiro
Alvo - Orçamentário
Alvo - Patrimônio
CheckList CCO
Check List do CCO

Painel do LOCMR para utilização nas TVs dos abrigos
SSA - Solicitação de Acesso às Áreas Operacionais
Sistema Visual de Aviso ao Público - SVAP
MIX - Avaliação de Desempenho
MIX - Treinamento
MixWeb - Dados Cadastrais
MixWeb - Gestão de Desempenho
MixWeb - Programação de Férias
MixWeb - Treinamento
Sistema de Controle dos Bicicletários
Sistema Público de Escrituração Digital (SPED FISCAL)
SSL - Sistema de Solicitação de Serviço em Laboratório
Alvo - Bancário
Alvo - Contabilidade
Alvo - Contas Públicas
Alvo - Contratos a Pagar
Alvo - Contratos a Receber
Custo da Ocorrência Operacional
Consulta dados da Frota
Aplicação de mapas da CPTM
Localização de Material Rodante no Mapa
MIX - Administração
MIX - Benefícios
MIX - Cargos e Salários
MIX - Controle de Equipamentos
MIX - Gerador de Eventos para Email
MixWeb - Afastamento
MixWeb - Cadastro de Vigilantes
Alvo - Cadastros Básicos
Alvo - Custos
AVC - Emissão de Avisos de Crédito
Bilhetagem
Gráfico Horário e Regularidade
MIX - Controle de Vagas
MIX - Jurídico
MIX - Medicina e Segurança
MixWeb - Benefícios
MixWeb - Consulta
MixWeb - Gerenciamento de Mensagens
MixWeb - Ordem de Serviço
Sistema de Recolhimento de Trens - RETREM
Segurança Ferroviária
SICOM Manutenção - Consulta Falha e OSM
SICOM Operação - Consulta Ocorrência Operacional
Análise de Ocorrência COPESE
Sistema de Desempenho da Circulação
MicroStrategy

BI.Indicadores Diretoria
CATPROD - Catálogo de Produtos
Sharepoint - Portal CPTM
Sharepoint.CPTM.Services
Sharepoint - Intranet On-Line (Azure Cloud)
SIEC - Sistema Informatizado de Engenharia de Custos
SESUITE - Processo
Sistema de Processos Integrados
SPI - Sistema Controle de Lixo
SPI - Gestão de Proposição
Avaliação do Aprendizado de Procedimentos de Operação - SAAPO
SE SUITE
BI - Indicadores de Manutenção Operacional
BI - Indicadores de Produção Operacional

15.3.2. SERVIÇOS DE MÉDIA CRITICIDADE:

Sistema
Serviço de publicação e manutenção de aplicação
CND - Controle de Numeração de Documentos
Atualização de Ocorrência COPESE
Monitoramento COVID-19
CPTM.ActiveDirectoryLibrary
Formulário COVID-19
CPTM.ComponentesLibrary
CPTM.CasisLibrary
DataRoom de Concessão
DataRoom Externo
Declaração de Ocorrência Operacional
SESUITE - Documento e Arquivo Físico
Documentos CPTM - SPI
Elmah ASP
Fale Conosco RH
CPTM.FCN.Service
Documentos CPTM - SPI - Externo
CPTM.GNULibrary
Gestão de Notificação de Usuário
Gestão de Editais de Licitações
Consulta de Editais de Licitações
Monitoramento de Equipamentos e Máquinas - WebAPI
Gerador de Números para Documentação
Tela de Acesso Negado
Dashboards (MicroStrategy)
MSTR_ETL.Service
Nexo
Nexo.Interface

Serviço de notificação para usuários de aplicações Web
Sharepoint - Office Social Bar
Painel de Comunicação Interna
Painel de Comunicação Interna
Painel de Comunicação Interna - WebAPI
PDI - Programa de Desligamento Incentivado
API com dados diversos para utilização pela GOAL
Portal CPTM em Período Eleitoral
Pesquisa de Satisfação de Atendimento
Pesquisa de Satisfação do Atendimento de chamados
Instrução de Serviço
MEC - Monitoramento de Equipe em Campo
Movimento de Embarque - Validações dentro e Fora do Diário Operacional
Portal CPTM - Central de Relacionamento
Sistema de Gestão de Documentação Administrativa
Sharepoint - ION
Sincronismo Oracle x Sharepoint Online
Sincronismo Oracle x Sharepoint OnPremise
Sistemas RH
Relatório de Serviço Diário do Maquinista ("X")
Votação Eletrônica CIPA
WAPI
WAPI.API
WAPI.Autenticacao
BI - Indicadores GFI
API com dados sobre a FROTA
Nexo.Agenda Médica
SPI - Controle de Metas Graficos
BI - Indicadores de Custos
BI - Indicadores de Segurança
Controle de Metas Operacionais
Indicação de Substituto Durante as Férias
SMS - CONTROLE - Controle de SMS da Segurança Operacional - Controle
Credencial de Desempregado
Cadastro de Foto - Perfil do Empregado
Gestão de Vistoria - Contratos Exploração Comercial
SMS - Controle de SMS da Segurança Operacional
Sistema de Localização
Metas Corporativas
SMS Denúncia - Integração Sistema Indicadores
RAIZ - Sistema Corporativo de Informações Georreferenciadas da CPTM
Sistema de Gerenciamento de Obras
SPI - Controle Aquisição e Contratação GFI
SPI - Áreas Comerciais
SPI - Controle de Metas (Desempenho)
SPI - Contratações e Compras
SPI - Controle de Correspondências DF

SPI - Jurídico Administrativo
Jurídico Arbitragem
SPI - Jurídico Cível
SPI - Jurídico Consultivo
SPI - Jurídico Criminal
SPI - Jurídico Licitações
SPI - Tribunal de Contas
SPI - Juridico Trabalhista
SPI - Controle Processos Segurança de Trabalho
SPI - Gestão Recomendações e Sindicâncias
SPI - Solicitação Serviços Administrativos
Sistema Gestão de Riscos
SP Sem Papel Consulta Interna
SMS Denúncia - Manutenção
SPI - Monitoramento Atividade
APP CPTM OFICIAL para Smartphones
SMS Denúncia - Integração Modem Daruma
Central de Denúncias
Componentes de Giro
Simulação de Carregamento de Passageiros
CPC - Controle de Processos de Custos
CPTM.CorreiosLibrary
Canal de Denúncias
Consultas do Diário Operacional
SMS Service WCF
SPI - Controle de Imagens e Requisições de Segurança
Venda Passagens Estrada Ferro Campos do Jordão EFCJ
Monitoramento de Equipes em Campo - WEBAPI
Nexo.Administração
Nexo.Gestão Previdenciária e Social
SVAP - WebAPI
Sistema de Pesquisa Gestores na Estação
SESUITE.WorkFlow
Seguranca
BI - Indicadores Posto Médico
Componentes de Giro
CPA - Simulação de Carregamento de Passageiros
Feedback Positivo
Nexo.Medicina do Trabalho
Nexo.Segurança do Trabalho
NexoWeb - Equipamento de Proteção Individual
Sistema de Análise e Gestão Ambiental
SCI - Sistema de Cadastro de Inventário
SPI - Gestão Ata
SPI - Controle SESMT Não Conformidades
SR - Sistema de Recomendações
Api da Segurança novo Modelo

Administração Organograma
Consulta Documentos Técnicos Operacionais
Controle de Inventário de Celulares
Controle de Inventário de Equipamento
Agente de Inventário de Equipanentos
Consulta Movimentação de Funcionário
CPTM.AspMail
CPTM.ComumLibrary
CPTM.ComumWebLibrary
CPTM.ImageRedim
CSICOM - Exportação de dados do SICOM
Diário Operacional
Documentos Deliberativos
Formulários
Gerador de Dígitos Verificador
Gestão de Notificação ao Usuário
GRD - Gestão de Reunião de Diretoria
Consulta Gerencial de Ocorrências do SICOM
Logística da Segurança Ferroviária - WebAPI
Manifestações de Usuários
Monitoramento de Equipamentos e Máquinas
Nexo.Indicadores
Obtenção de Fotos
Repositório do Conselho Fiscal, Administrativo e Estatutário
Repositório do Conselho Fiscal, Administrativo e Estatutário
Repositório de Documentos de Governança
SAQ - Sistema de Avaliação da Qualidade
Consulta de Escala de Sobreaviso
Sistema de Gestão de Acervo
SPI - Controle AVCB (Questionário)
Versionamento de Biblioteca de Operação

15.3.3. SERVIÇOS DE BAIXA CRITICIDADE:

Serão todos considerados os ambientes desenvolvimento, teste e homologação.

16. TRANSIÇÃO

16.1. OBJETIVOS GERAIS

O objetivo da fase de transição é mitigar os riscos inerentes da transferência dos serviços de um fornecedor para outro que se encontram dentro do objeto da contratação, conforme especificado neste Termo de Referência, considerando todos os seus aspectos (pessoas, processos, ferramentas, papéis e responsabilidades).

16.1.1. O plano de transição deve assegurar que tais tarefas sejam executadas adequadamente e que todas as partes envolvidas tenham uma clara compreensão de seu papel nesse processo. Cabe, portanto, a CONTRATADA descrever detalhadamente sua Abordagem de Transição, que será parte integrante da contratação, incluindo o modelo de gerenciamento a ser adotado, bem como os produtos gerados em cada etapa.

16.1.2. A fase de transição terá uma duração máxima de 30 (trinta) dias corridos a partir da emissão da Ordem de serviço pela CPTM.

16.1.3. O Projeto de Transição deve ser apresentado pela CONTRATADA à CPTM num período máximo de 5 (cinco) dias úteis após a formalização da contratação, contando com gerenciamento e equipe para absorção do conhecimento.

16.1.4. Durante a fase de transição a CONTRATADA deverá atuar atendendo ao objeto da CONTRATAÇÃO, mantendo o ambiente de TI da CPTM.

16.2. INÍCIO DO CONTRATO – EMISSÃO DA ORDEM DE SERVIÇO PELA CPTM

16.2.1. Abordagem de Transição deverá contemplar, no mínimo, os seguintes itens:

16.2.1.1. Juntamente com a CPTM, a CONTRATADA deverá identificar uma lista de “componentes de transição” (ex.:

ativos, localidades.) cobrindo a totalidade dos serviços de acordo com o objeto da contratação;

16.2.1.2. A CONTRATADA inspecionará, então, os “componentes de transição” e proverá a CPTM um “checklist” de transição (ex.: instalação de sistemas de monitoramento, estabelecimento das posições de atendimento ao usuário) para garantir uma transição tranquila;

16.2.1.3. A CPTM avaliará o “checklist”, a fim de aprovar formalmente o documento;

16.2.1.4. A CONTRATADA deverá executar uma inspeção final nos materiais e nas informações e requisitar esclarecimentos;

16.2.1.5. A CPTM deverá conduzir um programa de comunicação intensivo antes e durante a fase de transição, direcionado aos interessados envolvidos no processo (ex.: outros provedores, empregados, usuários) explicando o racional e o impacto do movimento em andamento. A CPTM pode, a qualquer momento, solicitar apoio da CONTRATADA para realizar esta atividade;

16.2.1.6. A CONTRATADA irá liderar as atividades da fase de transição. A CPTM proverá o suporte que a CONTRATADA eventualmente necessite para garantir uma transição tranquila e dentro dos prazos estipulados;

16.2.1.7. Durante o processo de transição, haverá reuniões periódicas da equipe de transição da CONTRATADA com a CPTM. Elas devem abranger:

16.2.1.7.1. Atividades de transição;

16.2.1.7.2. Revisão dos planos iniciais e alterações;

16.2.1.7.3. Análise de gaps (quebras de continuidade, disparidades.);

16.2.1.7.4. Gerenciamento de emissão e plano de ação;

16.2.1.7.5. Designação de recursos (equipamentos, mobiliários);

16.2.1.7.6. Designação das equipes efetivas em seus respectivos locais de trabalhos;

16.2.1.7.7. Data de resoluções;

16.2.1.7.8. Rota de superação dos obstáculos;

16.2.1.7.9. Plano de contingência para eventuais ocorrências que possam ocorrer;

16.2.1.7.10. Apresentar o planejamento estratégico de execução dos planos de contingência essenciais.

16.2.1.8. Além disto, a Abordagem de Transição deve considerar os seguintes requerimentos específicos:

16.2.1.8.1. A CONTRATADA deverá assumir a totalidade dos serviços requeridos, para cada disciplina, adotando o mesmo procedimento em todas as fases da transição, nas condições em que hoje se encontram o ambiente de TI da CPTM, a partir da emissão da Ordem de Serviço;

16.2.1.8.2. Na etapa inicial, de 60 (sessenta) dias a partir da emissão da Ordem de Serviço, não serão exigidos quaisquer movimentos ou ações no sentido de atender aos Acordos de Nível de Serviços (SLA), devendo a CONTRATADA envidar o máximo esforço para cumprir os SLA's definidos. Esta etapa é considerada como o período para estabilização da prestação dos serviços;

16.2.1.8.3. O Plano de Transição a ser proposto pela CONTRATADA deve ser complementado por um cronograma detalhado, contemplando todas as atividades, prazos, esforços, responsabilidades e entregáveis de cada fase ou atividade;

16.2.1.8.4. Durante a transição deverão ser elaborados os scripts dos atendimentos, como segue:

16.2.1.8.4.1. Os roteiros, levantamentos de processos e procedimentos atualmente existentes e em uso no ambiente de TI, com a finalidade de apresentar os procedimentos e desenhos de processos, ou seja, os scripts de atendimento dos serviços (também denominados roteiros) de TI, disponibilizando-os a CPTM;

16.2.1.8.4.2. A CPTM analisará os roteiros apresentados, validando-os. Os scripts não aprovados, incompletos ou que não atendam a finalidade ao qual se destinavam, deverão ser revistos e reapresentados em 48 horas úteis;

16.2.1.8.4.3. Os scripts serão integrados a base de conhecimento da ferramenta de atendimento ao usuário da CONTRATADA, após validação e aprovação;

16.2.1.8.4.4. A CPTM disponibilizará todas as informações necessárias para que a CONTRATADA elabore os scripts de atendimento.

16.3. ENCERRAMENTO DA FASE DE TRANSIÇÃO

16.3.1. Esta fase formaliza a finalização do Projeto de Transição através de seu aceite formal. Os entregáveis do projeto são avaliados e homologados pela CPTM. São registrados fatores positivos e negativos da realização do projeto, conhecido como Lições Aprendidas. A partir do encerramento do Projeto de Transição, as áreas de entrega da CONTRATADA são responsáveis por operar o ambiente no modo de SLA, mantendo a estabilidade e disponibilidade, procurando e promovendo mudanças na estrutura implementada de forma contínua.

16.4. ENCERRAMENTO DO CONTRATO (PHASE-OUT)

16.4.1. A CONTRATADA cujo contrato está se encerrando, deverá prestar auxílio e suporte à nova empresa que vier a ser a vencedora em um novo processo licitatório, por um período de até 30 dias, antes do encerramento do contrato, sem ônus adicional à CPTM. Cabendo à CONTRATADA alocar um contingente de profissionais que considere adequado para absorção do conhecimento e das atividades a serem transferidas pela empresa atual, pelo prazo de 30 dias antes do encerramento do contrato que será extinto, lembrando que a Ordem de Serviço será emitida para início das atividades após o término da transição aqui abordada.

16.4.2. A CPTM esclarece também que por ser um serviço continuado a transição não pode sofrer interrupção sob risco de descontinuidade ou prejuízo no nível dos serviços, o que implicará em prejuízo para a Administração Pública, com responsabilização a quem der causa.

16.4.3. A CPTM assegura que independentemente de vigência superpostas, que a execução do objeto somente ocorrerá por um dos contratados, não havendo possibilidade de acarretar pagamentos em dobro.

16.4.4. A CONTRATADA deverá devolver os crachás e documentos da CPTM em seu poder, ao término do contrato.

16.4.5. A CONTRATADA deverá apresentar a CPTM, um plano de transição de saída completo (Phase-out) dos serviços prestados ao término de sua contratação, de forma a estar claro como a CONTRATADA pretende e em qual prazo, realizar toda a migração dos serviços a nova empresa a ser CONTRATADA e/ou a CPTM.

16.4.6. Nesta fase a CONTRATADA deverá entregar relatórios comprobatórios a CPTM contendo status da tecnologia da CPTM, incluindo sua organização, hardware, software, aplicações específicas, funções vitais de negócio suportadas por TI, processo e/ou procedimentos a serem executados para garantia da operação do ambiente, base de conhecimento, base de chamados.

16.4.7. Tais atividades devem constar no plano de transição:

16.4.7.1. Análise da situação atual do serviço (ambiente, equipe, conhecimentos), para comprovar se está alinhado com a abrangência definida no contrato;

16.4.7.2. Checklist completo contendo todas as atividades e entregáveis do processo de transição;

16.4.7.3. Cronograma completo contendo todas as atividades, prazos e esforços necessários para o processo de transição;

16.4.7.4. Apresentação da medição dos níveis de serviço prestados e que estão sendo os contratuais no serviço regular;

16.4.7.5. Apresentação da documentação de forma clara que subsidie a abrangência dos serviços prestados;

16.4.7.6. Definição das relações entre todos os grupos internos e externos a serem envolvidos durante a fase de transição;

16.4.7.7. Descrição de como a informação deverá fluir entre os membros do projeto (plano de comunicação);

16.4.7.8. Identificação de eventuais riscos e problemas, bem como será a comunicação dos mesmos;

16.4.7.9. Preparar e disponibilizar toda a equipe alocada na operação vigente a disposição da equipe de transição para passagem de conhecimento e quaisquer outras informações/documentações que sejam pertinentes ao processo tecnológico e operacional da CPTM;

16.4.7.10. Apresentar plano de como será a condução da gestão interna e o modelo de relacionamento com a futura CONTRATADA, com o objetivo de garantir o nível de excelência e SLA do ambiente em fase de transição;

16.4.7.11. Apresentar como será toda a logística necessária a ser implementada durante a fase de transição (ferramentas, equipes, documentação).

17. PERFIL DOS PROFISSIONAIS

17.1.1. A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos no contrato;

17.1.2. Os profissionais deverão ser alocados presencialmente na CPTM;

17.1.3. Os recursos relacionados as atividades voltadas para Suporte a Firewall serão disponibilizadas de forma remota.

17.1.4. Todos os profissionais deverão possuir qualificação plena e conhecimento técnico compatível com a complexidade das demandas a serem atendidas;

17.1.5. Poderão ser aceitos, a critério da CPTM, prestadores de serviços que não atendam a todos os requisitos especificados no perfil, desde que a CPTM entenda ser o recurso possuidor de experiência para a execução das atividades e a CONTRATADA possua em seu quadro de funcionários prestadores capazes de suprir qualquer necessidade advinda destes conhecimentos;

17.1.6. Poderá haver casos em que será exigida a apresentação um plano de treinamento, a fim de adequar o recurso à necessidade do negócio. A solicitação do plano de treinamento, bem como sua aprovação ficará a critério da CPTM;

17.1.7. A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA;

17.1.8. Os profissionais deverão executar os procedimentos de acordo com as regras de segurança da informação;

17.1.9. Durante a execução dos serviços, a CONTRATADA se obriga, durante a execução do Contrato, a manter todos os profissionais com as qualificações especificadas.

17.1.10. A CONTRATADA e sua equipe técnica deverão se manter atualizadas nas evoluções tecnológicas do mercado, bem como estarem aptas a executar os serviços em novas ferramentas, metodologias, boas práticas, softwares e sistemas operacionais que venham a ser implantados nas instalações da CPTM;

17.1.11. Caso haja a implementação de novas tecnologias, plataformas, sistemas ou processos que impactem diretamente a execução dos serviços contratados, a CONTRATANTE será responsável por prover a capacitação necessária à equipe da CONTRATADA alocada para a operação dos referidos serviços, a fim de garantir a continuidade e a qualidade na prestação dos serviços. A capacitação será realizada dentro do prazo adequado e de forma compatível com a complexidade da nova tecnologia adotada, de modo a assegurar que a equipe da CONTRATADA esteja plenamente preparada para operar e manter as novas soluções implementadas.

17.1.12. A qualquer tempo, durante a vigência do contrato, a CPTM poderá solicitar que a CONTRATADA realize a apresentação dos certificados de conclusão escolar e curriculum vitae dos prestadores de serviço, bem como os certificados requeridos na descrição dos perfis, visando a comprovação de qualificação do profissional;

17.1.13. Em caso de férias de um profissional, a CONTRATADA deverá alocar profissional com as mesmas qualificações do profissional que sairá de férias, com no mínimo 5 (cinco) dias úteis antes do início do período de férias, para que haja a transmissão de conhecimento das atividades que deverão ser executadas.

17.1.14. Em caso de substituição de um profissional, a CONTRATADA deverá alocar profissional com as mesmas qualificações do profissional efetivo, com no mínimo 5 (cinco) dias úteis antes da saída desse, para que haja a transmissão de conhecimento das atividades que deverão ser executadas, excetuando casos em pedido de desligamento do próprio colaborador, com documentação apresentada a CONTRATANTE.

17.1.15. A não observância desta obrigatoriedade (alocação presencial dos profissionais, substituição em férias e substituição do profissional) implicará em penalidades definidas no contrato.

17.1.16. A CONTRATADA deve manter, durante todo o período de execução contratual, estrita aderência aos requisitos de perfis profissionais e de qualificação técnica da equipe.

17.1.17. A CONTRATADA deverá manter uma equipe técnica mínima, alocada no ambiente do CPTM, necessária à execução das atividades de 2º e 3º níveis.

17.1.18. É de total responsabilidade da CONTRATADA manter a coesão entre as equipes, garantindo melhoria contínua dos serviços prestados por meio de mapeamento, documentação e automação de serviços e processos.

17.1.19. Os profissionais de atendimento e suporte aos equipamentos de Firewall deverão ser disponibilizados gradativamente de acordo com o crescimento do parque da CPTM de Firewalls mediante alinhamento prévio entre CPTM e CONTRATADA, este alinhamento deverá ocorrer com no mínimo 120 dias de antecedência.

17.2. ANALISTA DE MONITORAMENTO – PRESENCIALMENTE NA CPTM

17.2.1. REQUISITOS PROFISSIONAIS

17.2.1.1. Formação: Nível Superior em TI (completo);

17.2.1.2. Experiência: 3 anos na área;

17.2.1.3. Certificação ITIL V4 ou superior;

17.2.2. CONHECIMENTOS

17.2.2.1. Conhecimento básico em Sistemas operacionais Linux;

17.2.2.2. Conhecimentos avançados em manutenção e configuração de ambientes Microsoft Windows 10 ou superior;

17.2.2.3. Conhecimentos em tecnologia de autenticação Active Directory;

17.2.2.4. Conhecimentos em Microsoft/Office 365 e pacote office 2016 ou superior;

17.2.2.5. Conhecimentos em redes de computadores, com e sem fio, protocolo TCP/IP, criptografia e segurança de rede wireless;

17.2.2.6. Inglês básico para leitura;

17.2.2.7. Conhecimentos em Microsoft Visio.

17.2.2.8. Conhecimentos na ferramenta de monitoramento Zabbix;

17.2.2.9. Conhecimento em suporte a sala cofre;

17.3. ANALISTA DE PROCESSOS – PRESENCIALMENTE NA CPTM

17.3.1. REQUISITOS PROFISSIONAIS

17.3.1.1. Nível Superior completo ou cursando nas áreas de Ciências Exatas, Engenharias, Administração, ou áreas afins;

17.3.1.2. Experiência: Mínimo de 2 anos na área de análise de processos ou melhoria contínua;

17.3.1.3. Certificação em BPM (CBPP, OCEB ou equivalente);

17.3.2. CONHECIMENTOS

17.3.2.1. Conhecimento em ferramentas e técnicas para Gerenciamento de Processos (BPMN, Lean Six Sigma, ou correlatos.);

17.3.2.2. Conhecimento em ferramentas de mapeamento e modelagem, como Microsoft Visio, Bizagi Modeler, ou Lucidchart;

17.3.2.3. Conhecimento em ferramentas de BI (Power BI, Tableau, QlikView);

17.3.2.4. Conhecimentos ITIL v4 Foundation ou superior;

17.3.2.5. Conhecimentos em Lean Six Sigma Yellow Belt ou superior;

17.4. ADMINISTRAÇÃO DE SERVIDORES WINDOWS I – PRESENCIALMENTE NA CPTM

17.4.1. REQUISITOS PROFISSIONAIS

17.4.1.1. Mínimo de 2 anos atuando em administração de servidores Windows;

17.4.1.2. Ensino superior completo ou cursando na área de Tecnologia da Informação ou correlatas;

17.4.1.3. Certificação ITIL V4 ou superior;

17.4.1.4. Certificação AZ-900 - Microsoft Azure

17.4.2. CONHECIMENTOS

17.4.2.1. Conhecimentos em soluções de backup;

17.4.2.2. Conhecimentos em ambientes de nuvem pública (Azure, AWS, GCP, OCI) e suas integrações com infraestrutura local (on-premises);

17.4.2.3. Bons conhecimentos em língua inglesa;

17.4.2.4. Conhecimentos em Microsoft Visio;

17.4.2.5. Conhecimentos na ferramenta de monitoramento Zabbix;

17.5. ADMINISTRAÇÃO DE SERVIDORES WINDOWS II – PRESENCIALMENTE NA CPTM

17.5.1. REQUISITOS PROFISSIONAIS

17.5.1.1. Ensino superior completo na área de Tecnologia da Informação ou áreas correlatas.

17.5.1.2. Mínimo de 4 anos atuando na administração de servidores Windows.

17.5.1.3. Certificação somente de produtos ativos e c/ suporte do fornecedor;

17.5.1.4. Certificação ITIL V4 ou superior;

17.5.1.5. Certificação AZ-800 - Administração da infraestrutura do núcleo híbrido do Windows Server;

17.5.2. CONHECIMENTOS

17.5.2.1. Conhecimentos em nuvem Pública (Azure, AWS, GCP e OCI);

17.5.2.2. Conhecimentos em software de backup Veritas Netbackup;

17.5.2.3. Conhecimentos em Appliance de backup Veritas;

17.5.2.4. Conhecimentos em NAS NetApp;

17.5.2.5. Bons conhecimentos em língua inglesa.

17.6. ADMINISTRAÇÃO DE SERVIDORES LINUX

17.6.1. REQUISITOS PROFISSIONAIS

17.6.1.1. Graduação em Tecnologia da Informação ou áreas correlatas;

17.6.1.2. Mínimo de 4 anos de experiência na administração de servidores Linux e ambientes de contêineres;

17.6.1.3. Certificação ITIL V4 ou superior;

17.6.1.4. Certificação LPIC-2 ou Red Hat Certified Engineer (RHCE) ou Suse Certified Engineer (SCE);

17.6.2. CONHECIMENTOS

17.6.2.1. Conhecimentos em Soluções de Backup;

17.6.2.2. Conhecimentos em Nuvem Pública (Azure, AWS, GCP e OCI);

17.6.2.3. Conhecimentos em Oracle Linux;

17.6.2.4. Bons conhecimentos em língua inglesa.

17.7. ADMINISTRAÇÃO DE VIRTUALIZAÇÃO/STORAGE – PRESENCIALMENTE NA CPTM

17.7.1. REQUISITOS PROFISSIONAIS

17.7.1.1. Graduação em Tecnologia da Informação ou áreas correlatas;

17.7.1.2. Mínimo de 3 anos de experiência em administração de virtualização e Storage;

17.7.1.3. Certificação ITIL V4 ou superior;

17.7.1.4. Certificação VMware Certified Professional - VCP e DELL Storage - Associate ou H13-611 Huawei Certified;

17.7.2. CONHECIMENTOS

17.7.2.1. Conhecimentos em nuvem Pública (Azure, AWS, GCP, OCI), Infraestrutura e Linux;

17.7.2.2. Conhecimentos em storages Dell Unity, Fujitsu AF, Huawei Dorado;

17.7.2.3. Conhecimentos em switches fiber channel Brocade;

17.7.2.4. Conhecimentos em NAS NetApp;

17.7.2.5. Conhecimentos em gestão de DHCP, DNS e IPAM Infoblox

17.7.2.6. Bons conhecimentos em língua inglesa.

17.8. ADMINISTRAÇÃO DE REDE NÍVEL I – PRESENCIALMENTE NA CPTM

17.8.1. REQUISITOS PROFISSIONAIS

17.8.1.1. Nível Superior em TI ou áreas correlatas, completo ou cursando;

17.8.1.2. Mínimo de 2 anos na área de administração de redes ou suporte técnico;

17.8.1.3. Certificação CCNA;

17.8.1.4. Certificação ITIL v4 Foundation ou equivalente;

17.8.2. CONHECIMENTOS

17.8.2.1. Conhecimentos em operação de switches de núcleo, distribuição, acesso e topo de rack em ambientes de datacenter;

17.8.2.2. Conhecimentos em infraestrutura de redes: Cabeamento estruturado, Roteadores, Switches e Access Point;

17.8.2.3. Conhecimentos em ferramentas de monitoramento e diagnóstico de rede (SolarWinds, Zabbix ou correlatos.);

17.8.2.4. Conhecimentos em firewalls Fortigate;

17.8.2.5. Conhecimentos em língua inglesa.

17.9. ADMINISTRAÇÃO DE REDE NÍVEL II – PRESENCIALMENTE NA CPTM

17.9.1. REQUISITOS PROFISSIONAIS

17.9.1.1. Nível Superior completo em TI ou áreas correlatas;

17.9.1.2. Mínimo de 3 anos na área de administração de redes;

17.9.1.3. Certificação CCNA;

17.9.2. CONHECIMENTOS

17.9.2.1. Conhecimentos em VOIP – Voz sobre IP;

17.9.2.2. Conhecimentos em operação e configuração de switches de núcleo, distribuição, acesso e Top-of-Rack em Data Centers;

17.9.2.3. Conhecimentos em ferramentas de monitoramento e diagnóstico de rede (SolarWinds, Zabbix);

17.9.2.4. Conhecimentos em infraestrutura de redes: Cabeamento estruturado, Roteadores, Switches e Access Point;

17.9.2.5. Conhecimentos em firewalls Fortigate;

17.9.2.6. Bons conhecimentos em língua inglesa.

17.10. ADMINISTRAÇÃO DE REDE NÍVEL III – PRESENCIALMENTE NA CPTM

17.10.1. REQUISITOS PROFISSIONAIS

17.10.1.1. Ensino superior completo em Tecnologia da Informação (TI) ou área correlata.

17.10.1.2. Mínimo de 4 anos na área de administração de redes.

17.10.1.3. Certificação ITIL V4 ou Superior;

17.10.1.4. Certificação CCNA ou CCNP Enterprise ou CCNP Collaboration ou CCNP Data Center ou CCNP Security;

17.10.2. CONHECIMENTOS

17.10.2.1. Conhecimentos em Switches de Núcleo, distribuição, Acesso e Topo de Rack em ambientes de Datacenter;

17.10.2.2. Conhecimentos Infraestrutura de redes: Cabeamento estruturado, Roteadores, Switches e Access Point;

17.10.2.3. Conhecimentos em de serviços de rede como DHCP, DNS e VPN;

17.10.2.4. Conhecimentos em ferramentas de monitoramento e diagnóstico de rede (SolarWinds, Zabbix);

17.10.2.5. Conhecimentos em Roteamento entre redes locais virtuais (VLANS), confecção e edição de listas de acesso (ACL), empilhamento de Switchs, agregação de portas, portas troncas, segurança de portas, prevenção de loops, análise de logs e monitoração SNMP;

17.10.2.6. Inglês nível avançado;

17.10.2.7. Conhecimentos em análise de logs e monitoração SNMP, com uso de ferramentas de monitoramento;

17.10.2.8. Conhecimentos básicos em firewall (FortiGate) e ferramentas de segurança de rede;

17.11. GESTÃO DE OPERAÇÕES DE TI – PRESENCIALMENTE NA CPTM

17.11.1. REQUISITOS PROFISSIONAIS

17.11.1.1. Ensino superior completo na área de TIC ou correlata;

17.11.1.2. Mínimo de 4 anos em gestão de operações de TIC;

17.11.1.3. Certificação ITIL V4 ou Superior;

17.11.1.4. Certificação desejável: ITIL Specialist (Create, Deliver & Support) 4;

17.11.1.5. Certificação desejável: COBIT 2019 ou superior;

17.11.2. CONHECIMENTOS

17.11.2.1. Conhecimentos em Infraestrutura de TIC: storages, virtualizadores, sistemas operacionais, bancos de dados, switches, redes LAN/WAN, segurança da informação e ambientes híbridos (on-premises e nuvem);

17.11.2.2. Conhecimentos em gerenciamento de Processos de Negócio (BPM);

17.11.2.3. Conhecimentos em normas de segurança da informação (ISO/IEC 27001);

17.11.2.4. Conhecimentos em práticas de gerenciamento de projetos baseadas no PMBOK.

17.11.3. EXPERIÊNCIA

17.11.3.1. Experiência comprovada em de liderar equipes multifuncionais;

17.11.3.2. Experiência comprovada em comunicação técnica e estratégica para elaboração de relatórios e apresentações;

17.11.3.3. Experiência comprovada em análise crítica para avaliação de processos e gestão de riscos;

17.12. ADMINISTRADOR DE BANCO DE DADOS ORACLE – PRESENCIALMENTE NA CPTM

17.12.1. REQUISITOS PROFISSIONAIS

17.12.1.1. Nível Superior completo em Ciências da Computação, Sistemas de Informação, Engenharia ou áreas afins;

17.12.1.2. Experiência mínima de 5 anos em administração de banco de dados Oracle;

17.12.1.3. Certificação Oracle Database Administration (OCA ou OCP) .

17.12.2. CONHECIMENTO

17.12.2.1. Conhecimento em Oracle Database 12c ou superior, Oracle RAC, Data Guard, e ambientes Disaster Recovery;

17.12.2.2. Experiência em Oracle Exadata e ambientes Multitenant (CDB/PDB);

17.12.2.3. Conhecimento em Oracle Enterprise Manager (OEM), Zabbix e backup/recovery com Oracle RMAN;

17.12.2.4. Sólidos conhecimentos em PL/SQL e tuning de desempenho;

17.12.2.5. Experiência com ASM (Automatic Storage Management) e ambientes Linux/Unix;

17.13. ADMINISTRADOR DE BANCO DE DADOS SQL

17.13.1. REQUISITOS PROFISSIONAIS

17.13.1.1. Nível Superior completo em Ciências da Computação, Sistemas de Informação, Engenharia ou áreas correlatas;

17.13.1.2. Experiência mínima de 5 anos em administração de banco de dados SQL Server;

17.13.1.3. Certificação MCSA SQL 2016 Database Administrator e ou DP-300 Azure Database Administrator Associate

17.13.2. CONHECIMENTO

17.13.2.1. Conhecimento em SQL Server 2016 ou superior e integração com Azure SQL Database;

17.13.2.2. Experiência com T-SQL e otimização de consultas;

17.13.2.3. Conhecimento em backup/recovery e SQL Server Management Studio (SSMS);

17.13.2.4. Experiência com SQL Server Data Tools (SSDT) e Azure Monitor;

17.13.2.5. Conhecimento em soluções de alta disponibilidade, como AlwaysOn e failover clustering;

17.14. ANALISTA DE SEGURANÇA DE PERÍMETRO EM REDES/FIREWALL

17.14.1. REQUISITOS PROFISSIONAIS:

17.14.1.1. Formação nível Superior em T.I

17.14.1.2. Experiência no mínimo de 08 anos na área

17.14.1.3. Desejável certificação ITIL 4 ou superior

17.14.1.4. Certificação em Firewall seja em CISCO, Fortinet, SonicWall, Palo Alto e/ou CheckPoint (desejável)

17.14.1.5. Inglês nível Intermediário

17.14.2. CONHECIMENTO

17.14.2.1. Conhecimentos em Sistemas Operacionais: Cisco IOS, FortiOS, F5 TMOS, CentOS, Ubuntu, SonicWall, CheckPoint

17.14.2.2. Conhecimentos em Active Directory / LDAP, TCP/IP (v4/v6), Autenticação MultiFator/Logon Único (SAML)

17.14.2.3. Conhecimentos em Certificados SSL/TLS, IDS/IPS, Firewalls de aplicativos da Web (CloudFlare ou Akamai)

17.14.2.4. Conhecimentos em proteção contra Spam de E-mail, Segurança IoT (melhores práticas)

17.14.2.5. Profundo conhecimento de Protocolos de Rede, tais como: WAN, VLANs, IPSEC, HSRP, BGP, RIP, OSPF, 802.11, QoS, DHCP, NTP, HSRP, VRRP, ARP, NAT, ACL,

Remote Access VPN, SIP, H.248, DNSSec, DKIM, NAC, NDR, EDR, XDR.

17.14.2.6. Conhecimento das vulnerabilidades em aplicação e mitigações conforme OWASP Top 10;

17.14.2.7. Conhecimentos em Switch: Cisco (STP, HSRP, SVI, EtherChannel, Stackwise, VSS, Nexus), WLAN Cisco, Cisco Meraki, Load Balancers, SD-WAN.

17.14.2.8. Conhecimentos avançados em tecnologias SDWAN

17.14.2.9. Ótima compreensão do modelo OSI e TCP/IP, Experiência prática com Ferramentas de Monitoramento, Diagnóstico e Análise de Redes (TCP Dump, Wireshark, NetCrunch ou correlatos).

17.14.2.10. Compreensão dos controles de segurança (por exemplo, controle de acesso, auditoria, autenticação, criptografia, integridade, criptografia, chave pública - infraestrutura).

17.14.3. EXPERIÊNCIA:

17.14.3.1.1. Experiência com gerenciamento de soluções de segurança de perímetro, incluindo firewall, VPN, IDS/IPS

17.14.3.1.2. Experiência de trabalho em soluções Fortigate, Cisco, CheckPoint, Sonicwall ou Watchguard

17.14.3.1.3. Experiência na elaboração de relatórios técnicos e procedimentos operacionais padrão.

17.14.3.1.4. Experiência em conceitos de rede como MPLS, TI/T3/E1, VoIP, Túneis de VPN, Deep Inspection, ou correlatos;

17.14.3.1.5. Experiência em Firewalls de Clouds Públicas (MS Azure/AWS Cloud/Google Cloud ou Oracle Cloud)

17.14.3.1.6. Experiência em produtos de segurança por exemplo, da FORTINET linhas; FortiNAC, FortiWEB, FortiADC e FortiGATE

17.14.3.1.7. Experiência com ferramentas de Teste de desempenho, como JMeter, Gatling ou LoadRunner

17.15. ANALISTA DE PROTEÇÃO DE ENDPOINTS (SEGURANÇA DE ANTIVIRUS) PRESENCIALMENTE NA CPTM

17.15.1. REQUISITOS PROFISSIONAIS:

17.15.1.1. Formação nível Superior em T.I;

17.15.1.2. Pós-Graduação e/ou MBA em Segurança da Informação, Cibersegurança e/ou correlatas;

17.15.1.3. Experiência no mínimo de 08 anos em TI;

17.15.1.4. Desejável certificação ITIL 4 ou superior;

17.15.1.5. Inglês nível Intermediário;

17.15.1.6. Conhecimentos indispensáveis em Normas: ISO 20000/27001, LGPD, Framework NIST CSF 2.0, MITRE ATT&CK®, OWASP Top 10;

17.15.2. CONHECIMENTO

17.15.2.1. Conhecimentos em melhores práticas, phishing e tipos de ataques;

17.15.2.2. Conhecimentos em Redes WAN, LAN, VLAN e protocolos de rede;

17.15.2.3. Conhecimentos em Criptografia, Análise de Vulnerabilidades;

17.15.2.4. Conhecimentos da Lei Geral de Proteção de Dados (LGPD);

17.15.2.5. Conhecimentos de hardening de SOs Windows e Linux;

17.15.2.6. Conhecimentos em Firewall, IDS/IPS, SIEM, Fator de Autenticação (MFA, OTP);

17.15.2.7. Conhecimentos de Segurança para ambientes em Cloud;

17.15.2.8. Conhecimentos em suporte a console de Antivírus Trendmicro, MS Defender, Kaspersky e/ou Crowdstrike;

17.15.2.9. Conhecimentos em NETWORK ATTACK DEFENSE - Prevenção de ataques provindos da rede baseado em táticas, técnicas e procedimentos do framework do MITTRE ATT&CK;

17.15.2.10. Conhecimentos em ANTI-RANSOMWARE - Defesa contra tentativas de ransomware criando automaticamente

um backup dos arquivos de destino que são restaurados após o bloqueio do malware;

17.15.2.11. Noções de Threat Hunting - Prática de investigação focada em determinar ameaças que podem prejudicar sistemas a partir de 3 critérios: Intenção, Capacidade e Oportunidade de causar danos;

17.16. GERENTE DE PROJETOS – PRESENCIALMENTE NA CPTM

17.16.1. REQUISITOS PROFISSIONAIS

17.16.1.1. Formação em nível superior completo em TI.

17.16.1.2. 03 anos de experiência em TI.

17.16.1.3. Conhecimento de Gerenciamento de Processos de Negócio (BPM).

17.16.1.4. Certificação em ITIL V3 (ou superior) Foundation.

17.16.1.5. Conhecimentos em COBIT Foundation.

18. PRAZO DE CONTRATAÇÃO

A contratação será por 30 meses, podendo ser aditada até o limite permitido pela legislação vigente.

19. MEDIÇÕES

19.1. Os serviços contratados serão apontados por medições mensais discriminados em relatório e deverão contemplar todos os serviços no período e aprovados pela CPTM.

19.2. Efetuar a entrega dos relatórios gerenciais (evidências do serviço prestado referente ao escopo desta contratação) no máximo até o quinto dia útil do mês subsequente ao mês da prestação dos serviços para aceite e atestação por parte da CONTRATADA dos serviços prestados;

19.3. As medições deverão indicar as quantidades correspondentes aos serviços prestados;

19.4. As medições deverão ser numeradas sequencialmente, discriminando o número do contrato, o seu objeto e o período de abrangência da mesma;

19.5. As medições deverão ser apresentadas ao GESTOR até o 5º dia útil, contado do último dia do período de adimplemento de cada obrigação, mediante protocolo que conste a data de sua entrega;

19.6. O GESTOR terá o prazo de 5 (cinco) dias úteis para a conferência da medição e a sua aprovação;

19.7. A medição não aprovada pelo GESTOR será devolvida à CONTRATADA para as necessárias correções, com as informações que motivaram a sua rejeição, contando-se o prazo estabelecido no subitem anterior, a partir da data de sua reapresentação;

19.8. A devolução da medição não aprovada pelo GESTOR, em hipótese alguma, servirá de pretexto para que a CONTRATADA suspenda a execução dos serviços;

19.9. Na hipótese de não pronunciamento pelo GESTOR quanto à medição no prazo definido anteriormente, considerar-se-á aprovada a medição;

20. CONDIÇÕES DE PAGAMENTO

20.1. A CPTM procederá ao pagamento nas condições previstas nesta cláusula.

20.2. O pagamento será realizado em 30 (trinta) parcelas mensais e iguais respeitando os demais subitens deste documento.

20.3. Após a aprovação da medição a CONTRATADA deverá, num prazo de até 02(dois) dias úteis, apresentar ao departamento fiscal da CPTM as vias originais da nota fiscal, das quais deverão constar todos os tributos incidentes na fonte sobre a prestação dos serviços, conforme estabelecido na cláusula de tributos descrito no edital, acompanhadas do respectivo documento de cobrança.

20.4. Na nota fiscal e no documento de cobrança deverão ainda ser indicados o número do contrato, o período medido e o número da medição.

No processo do pagamento, obedecerá a CPTM as disposições contidas na Lei nº 8.212, de 24 de julho de 1991, regulamentada pelo Decreto nº 3048, de 06 de maio de 1999 e demais normas pertinentes.

20.5. O documento de cobrança não aprovado pelo GESTOR será devolvido à CONTRATADA para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido a partir da data de sua apresentação.

20.6. A CPTM efetuará o pagamento no prazo de 30 (trinta) dias, a contar do último dia do período de adimplemento de cada parcela, desde que aprovados a medição, nota fiscal e documento de cobrança, nos prazos estabelecidos nas cláusulas de medição e de pagamento.

20.7. Na hipótese de ocorrer a devolução da medição, conforme previsto na correspondente cláusula, o prazo de pagamento será dilatado pelo número de dias contados entre a data de devolução e a (s) data (s) da nova apresentação.

21. ANEXO II – PLANILHA DE SERVIÇOS

Serviço	Unidade	Quantidade	Valor unitário	Valor total
Solução de Gestão do ambiente de TI	Mês	30		
Serviço de Coordenação de Operação de TI e Projetos	Mês	30		
Serviço Monitoramento de Ambiente de TI (NOC)	Mês	30		
Serviço de Gestão e Operação do Ambiente de Rede Corporativa	Mês	30		
Serviço de Administração e Operação de Banco de Dados	Mês	30		
Serviço de Gestão e Operação do Ambiente Virtualizado	Mês	30		
Serviço de Gestão e Operação de Soluções de Armazenamento	Mês	30		
Serviço de Gestão e Operação de Backup	Mês	30		
Serviço de Gestão e operação de segurança cibernética	Mês	30		
Solução de Firewall	Mês	30		
Solução estendida de detecção e resposta, segurança de endpoints e rede	Mês	30		
Total			**R$**	**R$**

ANEXO 2

CONTRATO DL00925-01 / PRODESP PD024401

PROPOSTA DA CONTRATADA

ANEXO II
ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS - ESP N.º E0240557

Este documento, a partir de sua assinatura, fará parte integrante do Contrato de Prestação de Serviços **PD024401,** firmado com a **COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM.**

1. OBJETO

Serviços técnicos especializados em gestão e operação de TI e Solução de cibersegurança.

2. ESCOPO DA PRESTAÇÃO DE SERVIÇOS

Estão contemplados os seguintes serviços para a solução:

- Solução de Gestão do Ambiente de TI;
- Serviço Técnicos Especializados em TI:
  - Serviço de coordenação de operação de TI e Projetos;
  - Serviço de monitoramento de ambiente de TI – NOC;
  - Serviço de gestão e operação do ambiente de rede Corporativa;
  - Serviço de administração e operação de Banco de Dados;
  - Serviço de gestão e operação do ambiente virtualizado;
  - Serviço de gestão e operação de soluções de armazenamento;
  - Serviço de gestão e operação de backup.
- Serviço de Segurança com Tratamento e Resposta à Incidentes Cibernéticos.
  - Solução de firewall:
    - ✓ Firewall as a service – FaaS;
    - ✓ Gerenciamento, análise de logs e emissão de relatórios.
  - Solução estendida de detecção e resposta, segurança de endpoints e rede:
    - ✓ Serviço de Proteção do Tráfego na Rede;
    - ✓ Serviço de Detecção e Resposta Estendida para Estações de Trabalho;
    - ✓ Serviço de Detecção e Resposta Estendida para Servidores;
    - ✓ Serviço de Proteção de Dados.
  - Serviços de gestão e operação de segurança cibernética:
    - ✓ Analista de Proteção de Endpoints;
    - ✓ Analista de Segurança de Perímetro em Redes/Firewall;
    - ✓ Governança.

2.1. Solução de gestão do ambiente de TI

2.1.1. Catálogo de Serviços – ativação até 40 atividades

Disponibilização de Interface web com o Catálogo de Serviços básico, composto por serviços de hardware / software padrão por meio do qual:

- Usuários finais (CONTRATANTE) solicitam serviços ou registram incidentes.

Obs.: o usuário que abre o chamado pode acompanhá-los por meio da ferramenta.

- Técnicos recebem as requisições de incidentes e solicitações reportadas, para dar andamento à solução dos pedidos de serviços.

2.1.2. Catálogo de Serviços - Ativação / Alteração Adicional

Refere-se às modificações no Catálogo de Serviços durante a vigência do contrato, abrangendo a inclusão de novas atividades, a alteração ou exclusão de atividades existentes ou ainda alterações nos workflows de aprovação

2.1.3. Manutenção do Cadastro de Dados

Alteração ou atualização dos dados dos usuários e técnicos, tais como e-mail, endereço, área, aprovador, etc, solicitado pelo próprio usuário ou pelo responsável do cliente, através de abertura de chamado

2.1.4. Console de Gerenciamento

Permissão de acesso dos técnicos para tratamento das requisições de serviços ou incidentes.

- Inclui 1 licença para até 03 analistas, não simultâneos *floatings* – por registro:
    - A licença pode ser utilizada por qualquer usuário, porém não de forma simultânea.
- Inclui 1 licença para até 01 analista, não simultâneo fixa – por registro:
    - A licença somente poderá ser usada pelo usuário que a detém, sem expirar.

2.1.5. Pré-requisitos

- Projeto de implantação da interface do sistema;
- Levantamento e carga inicial de dados de cadastro da CONTRATANTE referentes a usuários e estrutura organizacional (unidades ou departamentos), perfis/níveis de aprovação;

- Link Intragov ou acesso à Internet.

2.2. Serviço Técnicos Especializados em TI

Os serviços de Outsourcing de TI consistem na alocação de recursos técnicos profissionais variados, com o intuito de atender às necessidades de TI do ambiente da CONTRATANTE, desde suporte a usuários até administração de servidores, redes, recursos em nuvem, gestão de TI e projetos, entre outros.

Incluem serviços de:

- Operação, instalação e suporte a usuários;
- Operação, configuração, instalação e administração de ambientes de TI, podendo contemplar atividades de administração e gerenciamento de servidores, diretórios de usuários, serviços de impressão, redes, internet/INTRAGOV, banco de dados, backup, suporte a recursos aprovisionados em nuvem pública etc.

2.2.1. Serviço de coordenação de operação de TI

2.2.1.1. Atividades Previstas

- Acompanhar / viabilizar projetos de manutenção e instalações de soluções de TIC;
- Acompanhar, analisar e controlar a execução das atividades buscando a melhoria contínua nos pilares de capacidade, continuidade e disponibilidade da infraestrutura de TI;
- Alcançar melhoria e excelência na prestação dos serviços oferecidos através de processos baseados nas melhores práticas descritas pelo ITIL e auditados pelo COBIT;
- Aplicar conceitos de gestão da qualidade no atendimento, apoiando na gestão de Estratégias, Políticas e Padrões da Área de TIC;
- Apoiar os gestores na melhoria de uso das ferramentas, processos, gestão e alocação de recursos;
- Efetuar o planejamento e a gestão de capacidade dos elementos de infraestrutura necessários ao funcionamento dos serviços e soluções de TIC;
- Elaboração de atividades de melhoria contínua dos processos;
- Elaboração de relatórios de indicadores de desempenho da equipe e dos serviços prestados;
- Elaborar e recomendar melhorias nos fluxos de trabalho dos profissionais da CONTRATADA e da CONTRATANTE;
- Elaborar planos de ação para o desenvolvimento das atividades das áreas;
- Gestão do conhecimento e gerência eletrônica de documentos;
- Gestão e auditoria dos planos de continuidade de serviços de TIC;

- Manter atualizadas as versões de todos os softwares e de componentes dos serviços e soluções de TIC, bem como gerenciar as respectivas licenças de uso e outros mecanismos que assegurem a recuperação da instalação dos equipamentos centrais da rede e dos respectivos serviços;
- Participar de reuniões, elaborar relatórios técnicos;
- Promover a visão de Gerenciamento de Serviços para todos os níveis;
- Promover, orientar e acompanhar, no que se refere à TIC, a implementação de Políticas Corporativas;
- Realizar contatos telefônico/pessoal com fornecedores e/ou clientes e internos/externos;
- Promover, orientar e acompanhar ações voltadas às práticas de Segurança da Informação e gestão de risco na gestão de operações;
- Implementar processos de requisições, incidentes, problemas e mudanças utilizando principais práticas de mercado;
- Implementar/operar sistemas de Gerenciamento de Serviços de TIC (ITSM) para registro e acompanhamento de requisições, incidentes, problemas e mudanças do ambiente.

2.2.1.2. Disponibilidade

- O serviço será oferecido em horário comercial, das 9h às 18h, de segunda a sexta-feira, com suporte emergencial em regime de sobreaviso 24x7x365.

2.2.2. Serviço de monitoramento de ambiente de TI – NOC

A CONTRATADA será responsável por operar um Centro de Operações de Rede (NOC) para monitorar continuamente a infraestrutura de TI da CPTM, garantindo a disponibilidade dos ativos e serviços. O serviço inclui detecção proativa de incidentes, uso de ferramentas especializadas, registro automático de falhas, atuação técnica imediata quando possível, e implementação de melhorias e automações.

2.2.2.1. Atividades Previstas

- Monitoramento contínuo (24x7x365) da infraestrutura de TI, incluindo servidores, redes, sistemas e serviços críticos;
- Detecção proativa de incidentes, com base em parâmetros e métricas previamente definidos;
- Utilização de ferramentas especializadas de monitoramento e diagnóstico, fornecidas e mantidas pela CONTRATADA;
- Registro automático de incidentes na Solução de Gerenciamento de Serviços de TI da CPTM;

- Atuação técnica imediata para resolução de incidentes de baixa complexidade, conforme scripts e procedimentos autorizados;
- Mapeamento contínuo de melhorias nos processos e ferramentas de monitoramento;
- Implementação de automações com base em matriz de decisão, visando maior eficiência operacional;
- Proposição e execução de rotinas automatizadas para testes de disponibilidade, desempenho e validação pós-mudança;
- Elaboração de plano de ação durante a fase de transição operacional, com foco na automação do monitoramento;
- Acompanhamento de fornecedores, quando necessário, para resolução de incidentes ou melhorias.

2.2.2.2. Itens Fora do Escopo

- Fornecimento de hardware ou licenciamento de software da infraestrutura;
- Treinamento ao usuário.

2.2.2.3. Disponibilidade

- O serviço será oferecido em regime de 24 X 7, durante os 365 dias do ano.

2.2.3. Serviço de gestão e operação do ambiente de rede

2.2.3.1. Atividades Previstas

- Administração e suporte aos ativos de rede e comunicação, abrangendo dados, voz, vídeo, videoconferência, LAN e Wireless;
- Análise de GAPs nos ambientes, com identificação de falhas e proposição de soluções técnicas e administrativas;
- Proposição e execução de melhorias contínuas no ambiente de rede.
- Orientação técnica às equipes de suporte sobre dispositivos e ambientes LAN;
- Acompanhamento da equipe de infraestrutura em serviços de manutenção de lógica e telefonia (convencional ou IP);
- Instalação e remanejamento de elementos ativos de rede e backbones.
- Instalação e remanejamento de Access Points de rede sem fio;
- Instalação física e remanejamento de servidores e racks, assegurando a conectividade e funcionalidade da rede;
- Adequações de cabeamento estruturado no Data Center, com materiais fornecidos pela CONTRATANTE (excluindo certificação de cabos e fusão de fibra óptica);

- Adequações no sistema estruturado do backbone e Data Center via fibra óptica, com materiais fornecidos pela CONTRATANTE (também excluindo certificação e fusão);

2.2.3.2. Itens Fora do Escopo

- Certificação de cabos de rede e fusão de fibra óptica;
- Fornecimento de materiais e equipamentos;
- Treinamento ao usuário;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções e sistemas de telefonia analógica / TDM;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções e sistemas de segurança / Firewalls;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções e sistemas de segurança eletrônica / CFTV;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções e sistemas de sonorização;
- Instalação de infraestrutura de redes / cabeamento óptico / metálico estruturado;
- Suporte a sistemas de alimentação elétrica / Geradores;
- Elaboração de Contratos, Atas, ou Projetos de Redes;
- Fornecimento de qualquer tipo de certificado digital.

2.2.3.3. Disponibilidade

- O serviço será oferecido em horário comercial, das 7h às 19h, de segunda a sexta-feira, com suporte emergencial em regime de sobreaviso 24x7x365.

2.2.4. Serviço de administração e operação de banco de dados

A CONTRATADA será responsável por administrar, operar, dar suporte e promover a evolução dos bancos de dados Oracle e Microsoft SQL Server da CPTM, garantindo a integridade, disponibilidade, desempenho e segurança dos ambientes, atuando de forma preventiva e corretiva.

As atividades abrangem desde a criação de normas e documentação técnica até a execução de rotinas de manutenção, monitoramento, tunning, migração, atualização e suporte emergencial, sempre em integração com as áreas de desenvolvimento, infraestrutura e negócios da CPTM.

2.2.4.1. Atividades Previstas

- Elaboração, implantação e manutenção de normas e procedimentos de administração de dados e SGBD.

- Instalação, customização, administração e manutenção dos SGBDs Oracle e MS SQL Server.
- Análise de GAPs e proposição de melhorias nos ambientes de banco de dados.
- Desenvolvimento e manutenção de rotinas de consulta, atualização e armazenamento de dados.
- Monitoramento de desempenho e disponibilidade dos bancos de dados, clusters e servidores.
- Definição e execução de rotinas de ETL (alimentação e extração de dados).
- Integração com equipes de desenvolvimento e manutenção de sistemas.
- Atualização de ambientes (produção, homologação, desenvolvimento) via gestão de mudanças.
- Documentação técnica dos bancos de dados, arquitetura, processos e produtos.
- Elaboração de relatórios consolidados de capacidade, desempenho e eventos.
- Gerenciamento de permissões de acesso e segurança.
- Análise e implementação de novos projetos e serviços, incluindo hardening e planejamento de capacidade.
- Manutenção corretiva e preventiva, incluindo recuperação de backups.
- Migração de versões e ambientes de banco de dados.
- Suporte técnico emergencial 24x7x365.
- Levantamento completo do ambiente computacional, incluindo servidores, sites, contingência, e diagnóstico de problemas.
- Apoio técnico em ferramentas específicas e atividades que exijam conhecimento de negócio.
- Participação em reuniões de GMUD e submissão de customizações para aprovação.
- Geração de relatórios de atividades e apoio à medição contratual.

2.2.4.2. Itens Fora do Escopo

- Fornecimento de hardware, licenças de software ou infraestrutura física;
- Desenvolvimento de stored procedures, funções e programas de rotina (responsabilidade da CONTRATANTE ou suas contratadas);
- Atividades fora do escopo do ambiente de banco de dados que envolvam aquisição de hardware;
- Treinamento ao usuário;
- Suporte, operação e manutenção de aplicações/sistemas;
- Elaboração de projetos de ambientes de OLAP (Data Warehouse, Data Lake, etc), nas suas diversas formas de ingestão de dados;
- Modelagem de dados/elaboração de relatórios com dados de negócio;

- Fornecimento de qualquer tipo de certificado digital.

2.2.4.3. Disponibilidade

- O serviço será oferecido em horário comercial, das 7h às 18h, de segunda a sexta-feira, com suporte emergencial em regime de sobreaviso 24x7x365

2.2.5. Serviço de gestão e operação do ambiente virtualizado

A CONTRATADA será responsável pela gestão e operação do ambiente virtualizado da CONTRATANTE, assegurando sua continuidade, desempenho, segurança e escalabilidade. O serviço abrange servidores, storages, redes virtuais e demais componentes da infraestrutura virtual.

2.2.5.1. Atividades Previstas

- Instalar, atualizar, configurar, customizar e suportar todos os servidores físicos e virtuais, sistemas operacionais e sistemas de virtualização que compõe a infraestrutura do datacenter do CPTM;
- Criar procedimentos de correção de falhas que serão adotados pela equipe do Monitoramento (NOC);
- Diagnosticar e resolver problemas de desempenho nos ambientes suportados;
- Verificar periodicamente os logs dos servidores, sistemas de storages e virtualização de modo a agir proativamente em casos de problemas ou comportamentos não esperados;
- Abrir e acompanhar chamados técnicos dos fabricantes das soluções instaladas;
- Implementar e Administrar serviços cluster e webserver (IIS, Apache);
- Realizar mudanças de configuração, novas configurações, novas implantações e todas as atividades necessárias, nos ambientes suportados, de modo a atender plenamente os serviços de TI da CPTM;
- Projetar, implantar e validar procedimentos de alta disponibilidade;
- Acompanhar o uso de recursos físicos pelo ambiente de virtualização, agindo proativamente, antes do esgotamento de recursos físicos dele;
- Efetuar instalação e atualização de aplicações nos ambientes mantidos pela CPTM, incluindo a atualização, deploy de aplicações e instalação ou configuração de componentes, seguindo procedimentos elaborados pelos serviços de administração e suporte aos servidores de aplicação, e aprovados pelo processo de habilitação de mudança da CPTM;
- Realizar a criação de políticas de grupos de operação, de backup, de alertas, de gerenciamento de espaço, de governança de dados dos produtos Microsoft adquiridos pela CPTM;

- Configurar permissões de usuários e/ou grupo dos produtos Office/Microsoft 365;
- Realizar a abertura e acompanhar chamados para suporte do fabricante sobre as ferramentas do Office/Microsoft 365 e suporte Unified da Microsoft.
- Atender a solicitações de arquiteturas, permissões de acesso do Office/Microsoft 365;
- Manter controle e padronização das configurações dos servidores de aplicação em uso na CPTM;
- Verificar, diariamente, se as tarefas estão sendo executadas de acordo com os níveis de serviço contratados;
- Analisar o ambiente utilizando métricas de desempenho, assegurando a continuidade, escalabilidade e desempenho adequado;
- Realizar análises de GAP nos ambientes, identificando falhas administrativas e propondo melhorias e soluções aplicáveis;
- Executar tarefas administrativas gerais, incluindo, mas não se limitando, a criação e gerenciamento de usuários, permissões de acesso, manutenção de logs, auditorias e configuração do firewall do Windows para bloqueios;
- Administrar File Servers Microsoft, utilizando recursos como ACL's, ABE, Shadow Copy e cotas de disco;
- Gerenciar e configurar Microsoft AD DC (incluindo instalação, configuração de GPOs, gerenciamento de replicações inter-sites, relação de confiança entre domínios, e criação de AD RODC);
- Aplicar atualizações de segurança recomendadas para sistemas operacionais, mantendo a estabilidade e o funcionamento ideal;
- Garantir backups regulares e restauráveis para proteção de dados em caso de falhas;
- Responder a incidentes e alertas, implementando soluções de contorno e propondo soluções definitivas;
- Configurar a coleta de dados de performance com Perfmon para indicadores críticos;
- Realizar o planejamento de capacidade para ambientes de servidores Windows, otimizando recursos;
- Desenvolver scripts em Batch, VBS e PowerShell para automação de processos administrativos;
- Elaborar e manter documentações técnicas detalhadas sobre servidores, serviços e infraestrutura, incluindo topologias e configurações;
- Implementar serviços Microsoft NLB para balanceamento de carga;
- Instalar, configurar e desativar servidores e softwares relacionados;
- Configurar e manter serviços essenciais tais como: DHCP, DNS, IIS, WSUS, Print Server, Microsoft Failover Clustering e AD CS;
- Projetar, implementar e manter ambientes híbridos, integrando soluções on-premises com nuvens públicas;

- Auxiliar nos testes de backup e restore, e efetuar o restore de todos os serviços inerentes à rede e Windows Server;
- Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com serviços de operação do ambiente de Virtualização;
- Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com os sistemas operacionais Microsoft;
- Atender e dar suporte de 3º Nível a incidentes, problemas e solicitações relacionados com sistemas operacionais baseados em Linux;
- Executar mudanças, migrações, atualizações, implantações e testes de novos produtos na plataforma Linux.
- Executar serviços nos servidores Linux, tais como gerenciamento de discos, parametrização dos sistemas, atualização de versões dos sistemas operacionais e aplicativos, aplicação de correções e patches.
- Gerenciar e manter a administração dos serviços de DNS, DHCP e Gerenciamento de IPs através da ferramenta INFOBLOX, mantida pela CPTM;
- Analisar e implementar ações de hardening;
- Manter base de conhecimento de procedimentos técnicos atualizados;
- Acompanhar fornecedores quando necessário;

2.2.5.2. Itens Fora do Escopo

- Fornecimento de licenças de software, hardware ou infraestrutura física.
- Execução de projetos de virtualização sem planejamento e aprovação prévia;
- Treinamento ao usuário;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções e sistemas de segurança / Firewalls;
- Instalação, configuração, gerenciamento, monitoramento e suporte de soluções de segurança para Endpoints (antivírus);
- Suporte técnico à usuários, administração de sistemas gerenciadores de banco de dados (SGBD), desenvolvimento de softwares/sistemas, treinamento a usuários;
- Suporte, operação e manutenção de aplicações/sistemas;
- Fornecimento de qualquer tipo de certificado digital.

2.2.6. Serviço de gestão e operação de soluções de armazenamento

Prestação de serviços especializados para a gestão, operação e manutenção das soluções de armazenamento da CONTRATANTE, abrangendo ambientes SAN e NAS, tanto on-premises quanto em nuvem.

O serviço inclui a administração de storages, configuração de volumes e LUNs, análise de desempenho, aplicação de boas práticas de segurança e suporte técnico especializado. A atuação será integrada às áreas de infraestrutura e

sistemas da CONTRATANTE, com foco em continuidade operacional e melhoria contínua.

2.2.6.1. Atividades Previstas

- Administração e manutenção de redes SAN e soluções NAS (iSCSI, NFS, CIFS);
- Análise de GAPs e proposição de melhorias técnicas.
- Configuração de multipathing, zoning, LUNs, volumes, RAID, snapshots e storag pools;
- Atualização de software e firmware dos storages, com análise de risco quando necessário;
- Monitoramento de desempenho, capacidade, consumo e saúde dos storages;
- Gerenciamento de cotas, Qtrees, sistemas de arquivos e crescimento de dados;
- Implementação de ações de hardening, tuning, balanceamento de carga e alta disponibilidade;
- Documentação técnica do ambiente de armazenamento;
- Acompanhamento de fornecedores e suporte técnico escializado;
- Manutenção da base de conhecimento atualizada;

2.2.6.2. Itens Fora do Escopo

- Fornecimento de hardware, licenças de software ou infraestrutura física.
- Suporte a aplicações hospedadas nos storages;
- Execução de atualizações sem aprovação formal da CONTRATANTE;
- Treinamento ao usuário.

2.2.7. Serviço de gestão e operação de backup

Prestação de serviços especializados para a gestão, operação e manutenção da solução de backup da CONTRATANTE. A CONTRATADA será responsável por garantir a continuidade, segurança, desempenho e confiabilidade das rotinas de backup e recuperação de dados, conforme a Política de Backup vigente.

O serviço abrange desde a criação e atualização de planos de backup até a execução de testes de restauração, análise de logs, aplicação de boas práticas e suporte técnico especializado. A atuação será integrada às áreas de infraestrutura e segurança da informação da CONTRATANTE.

2.2.7.1. Atividades Previstas

- Criação, implantação, manutenção e atualização dos planos de backup.
- Análise de GAPs e proposição de melhorias nos processos de backup.

- Configuração de jobs, políticas de backup/restore, deduplicação e agentes de backup.
- Execução de testes de restauração conforme frequência definida pela CONTRATANTE.
- Análise de logs e relatórios técnicos das rotinas de backup e restore.
- Movimentação de cópias entre datacenters e alteração de retenções.
- Aplicação de boas práticas de segurança, desempenho e alta disponibilidade.
- Criação, alteração e exclusão de rotinas de backup.
- Implantação e manutenção da estrutura de backup.
- Limpeza de logs obsoletos conforme política vigente.
- Recuperação de dados cobertos pelos planos de backup.
- Acompanhamento de fornecedores quando necessário.
- Elaboração e atualização da documentação técnica da solução.
- Manutenção da base de conhecimento atualizada

2.2.7.2. Itens Fora do Escopo

- Fornecimento de hardware, licenças de software ou infraestrutura física.
- Suporte a aplicações fora do escopo da solução de backup.
- Execução de atividades sem aprovação formal da CONTRATANTE.
- Treinamentos formais para equipes da CONTRATANTE (exceto se contratualmente previstos)
- Desenvolvimento de sistemas ou aplicações;

2.2.8. Serviços fora de escopo

- Infraestrutura e aplicação de informação da CPTM;
- Infraestrutura para integração com mainframe;
- Suporte à hardware (Reparo em servidores, *switches* e demais equipamentos de infraestrutura);
- Manutenção predial;
- Manutenção de infraestrutura de salas técnicas (Ar condicionado, rede/circuitos elétricos, *no-breaks*, geradores, etc);
- Operação, suporte e manutenção de:
    - Solução CFTV (Hardware e software);
    - Catracas;
    - Cancelas;
    - PABX TDM (Telefonia em geral);
    - Fornecimento de ferramentas, equipamentos, materiais e softwares, exceto computadores para profissionais alocados com o pacote MS Office.
- Elaboração e definição de políticas relacionadas à segurança da informação;

- Fornecimento ou substituição de hardware e software;
- Suporte a soluções de firewall de código aberto (open source);
- Serviços de suporte aos desktops e usuários (service desk);
- Desenvolvimento e manutenção de aplicativos e sistemas;
- Fornecimento de licenças de software em geral, exceto aqueles já contemplados nos serviços contratados;
- Suporte para utilização e reparos de software;
- Infraestrutura em geral;
- Manutenção de hardwares e ativos do cliente; Intervenções estruturais (paredes, telhados, teto, forros, instalações elétricas, cabeamento de rede), ou áreas de periculosidade;
- Implantação e administração de ambientes de BI (business intelligence);
- Quaisquer outras atividades não explicitadas neste RPT;
- Administração da plataforma Lotus Notes;

2.3. Serviço de Segurança com Tratamento e Resposta à Incidentes Cibernéticos

2.3.1. Soluções de Firewall

2.3.1.1. Firewall as a service – FaaS;

A solução de firewall como serviço (firewall as a service – FaaS) oferece um next-generation firewall (NGFW), que consiste numa barreira de proteção, com abordagem inteligente e proativa, que defende as camadas de rede contra ameaças cibernéticas avançadas.

O FaaS combina inspeção profunda de pacotes, controle de aplicações e prevenção contra intrusões, oferecendo uma proteção robusta e adaptável a todos os ambientes.

2.3.1.2. Gerenciamento, análise de logs e emissão de relatórios.

Plataforma de gerenciamento de logs, análises e relatórios que fornece aos clientes uma console único para gerenciar, automatizar, orquestrar e responder, permitindo operações de segurança simplificadas, identificação e remediação proativas de riscos e visibilidade completa de todo o cenário de ataques.

2.3.1.3. Atividades previstas

As equipes de segurança podem monitorar e gerenciar alertas e logs de eventos processados e correlacionados em um formato que os analistas podem entender facilmente. As visualizações fornecem insights profundos com contexto e significado da atividade da rede, riscos, vulnerabilidades, tentativas de ataque,

indicadores de comprometimento e anomalias, e atividades de usuários autorizadas e não autorizadas.

As atividades do suporte compreendem:

- Configuração e operação dos elementos que constituem o sistema de Firewall;
- Realização de backup lógico das configurações de Firewall;
- Gestão de credenciais de acesso ao Firewall;
- Criação, alteração ou exclusão de configurações definidas e autorizadas pelo cliente:
- Regras de Firewall;
- Perfis de acesso à Internet;
- Perfis de acesso VPN.
- Análise de logs e eventos gerados pelo Firewall;
- Aplicação de patches de correção e segurança
- Suporte e diagnóstico em conjunto com outras equipes para assuntos que envolvam configurações ou ajustes no Firewall;
- Acompanhamento das ocorrências, aplicação de contramedidas e comunicação ao CLIENTE sobre tentativas de invasão detectadas no Firewall;
- Elaboração de relatórios com informações sobre atividades realizadas e indicadores relacionados aos componentes que compõem o sistema de Firewall);
- Elaboração de relatórios com informações sobre atividades realizadas e indicadores relacionados aos componentes que compõem o sistema de Firewall (Mediante alinhamento e definição de um modelo padrão).

2.3.1.4. Entregáveis

- Relatórios Personalizados mediante definição de um modelo padrão:
- Criação de dashboards e relatórios automáticos para conformidade;
- Exportação em vários formatos;
- Correlações de Segurança;
- Relaciona diferentes tipos de eventos para detectar incidentes complexos;
- Gestão de Incidentes;
- Integração com SIEM e SOAR para resposta rápida;
- Sistema de tickets e acompanhamento.

2.3.1.5. Atendimento aos chamados de gerenciamento e monitoramento

Os chamados abertos serão atendidos de acordo com a severidade dele.

Durante a abertura do chamado, o cliente deverá informar a severidade do chamado que será ratificada ou retificada pelo especialista da PRODESP.

Severidade	Descrição
Severidade 1	Ambiente ou Equipamento parado
Severidade 2	Ambiente impactado
Severidade 3	Solicitação sem impacto no ambiente
Severidade 4	Dúvidas

Severidade 1 – regime 24x7

- Primeiro contato: até duas horas após a abertura do chamado.
- Solução de contorno: até seis horas após a abertura do chamado.
- Resolução: até dezesseis horas após a abertura do chamado.

Severidade 2 – regime 24x7

- Primeiro contato: até duas horas após a abertura do chamado.
- Solução de contorno: até oito horas após a abertura do chamado.
- Resolução: até vinte e quatro horas após a abertura do chamado.

Severidade 3 – regime 8x5

- Primeiro contato: até quatro horas em horário comercial após a abertura do chamado.
- Solução de contorno: até doze horas em horário comercial após a abertura do chamado.
- Resolução: até trinta e seis horas em horário comercial após a abertura do chamado.

Severidade 4 – regime 8x5

- Primeiro contato: até quatro horas, em horário comercial, após a abertura do chamado.
- Solução de contorno: nbd – next business day
- Resolução: até 48 horas, em horário comercial, após a abertura do chamado.

2.3.1.6. Disponibilidade

- O serviço de monitoramento estará disponível em período integral (24 horas × 7 dias por semana) e de forma remota .
- O serviço de gerenciamento estará disponível de segunda a sexta-feira, entre 07:00hs e 19:00hs.

2.3.1.7. Exceções

Em exceções, que envolvam problemas físicos nos produtos com necessidade de troca de hardware ou a intervenção do próprio fabricante para resolução do chamado, tais como alteração / atualização do Sistema Operacional do equipamento, a contagem do SLA será interrompida, até que a atuação do fabricante seja finalizada.

Abertura de chamado técnico junto ao suporte técnico do fabricante devido problemas de BUG ou incompatibilidade com equipamentos e softwares de terceiros a contagem de SLA deverá ser suspensa;

Caso a CONTRATANTE não autorize a realização de alguma atividade durante o processo de troubleshooting para a detecção e resolução do problema a contagem do SLA deverá ser interrompida;

Para que seja possível a abertura de chamados técnicos no suporte do fabricante, atualizações de software são necessárias para que todos os produtos que fazem parte do escopo deste contrato tenham um suporte válido com seus respectivos fabricantes.

2.3.2. Solução estendida de detecção e resposta, segurança de endpoints e rede

Solução de proteção para a rede coorporativa abrangendo soluções para estações de trabalho, notebooks, desktops, servidores, verificação de usuários e dispositivos, microsegmentação, inspeção contínua e bloqueio de tráfego suspeito integrada à plataforma de detecção e resposta estendida.

Esta solução é composta por:

2.3.2.1. Serviço de Proteção do Tráfego na Rede;

Inspeção avançada de ameaças a nível de rede integrada à plataforma de detecção e resposta estendida, incluindo a análise e mapeamento de ameaças no tráfego norte-sul e leste-oeste. Realiza a identificação de interlocuções cibercriminosas mapeando comportamentos anômalos na rede, frente a ataques de exploração de vulnerabilidades, movimentações laterais suspeitas e comprometimento de usuários.

Este serviço contempla:

- 1 x Appliance físico com capacidade de inspeção de até 4 Gbps.

Atividades Previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos a nível de rede.

Entregáveis

- Relatórios contemplando evidências de monitoramento e alertas tratados.

Pré-requisitos

Lista de pré-requisitos exigidos para cada appliance físico implantado:

- 1 x interface de rede com endereço IP disponível;
- 1 x interface de rede dedicada para espelhamento de porta no switch core ou distribuição;
- 1 x espaço em rack 2 U;
- 2 x alimentação estabilizada para energia AC (padrão americano);
- 1 x cabo de rede RJ45 ou fibra óptica.

Suporte Técnico

- O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;
- Horário de Atendimento: De segunda a sexta-feira, 8 horas por dia (entre 08:00hs e 17:00hs).

2.3.2.2. Serviço de Detecção e Resposta Estendida para Estações de Trabalho;

Solução de proteção para estações de trabalho, notebooks e desktops, integrada à plataforma de detecção e resposta estendida.

Este serviço contempla:

- 3200 agentes de Endpoint Security (Essentials)
- Proteção avançada baseada em machine learning (aprendizado de máquina - é um método de análise de dados que automatiza a construção de modelos analíticos);
- Identificação de ameaças baseada em análise comportamental;
- Detecção de ataques em memória;
- Antimalware de próxima geração;
- Bloqueio de ameaças via web reputation;
- Firewall de host (firewall em software que realiza o bloqueio de tráfego indesejado no dispositivo do usuário);
- Controle de aplicações;
- Identificação e blindagem de vulnerabilidades;
- Autoproteção do agente;
- Controle de dispositivos externos (USB, pen drive, HD externo);

- Endpoint detection and response – EDR (Detecção e Resposta de Endpoint);
- Integração nativa com a plataforma de detecção e resposta estendida.

Atividades Previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;
- Administração centralizada da plataforma de detecção e resposta estendida:
- Atualização automática do software de segurança;
- Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas nas estações de trabalho e servidores;
- Auxílio para solucionar as ocorrências de vírus, malwares e exploits;
- Identificação de ameaças ou suspeita de contaminação do ambiente corporativo;
- Comunicação de incidências de vírus e de ameaças de computador desconhecidas.

Entregáveis

- Relatórios contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas, potenciais vulnerabilidades presentes em endpoints;
- Relatório de TOP usuários, dispositivos e aplicações com risco;
- Relatório TOP hosts afetados por ameaças.

Pré-requisitos

- Sistema Operacional:
  Windows 10 (32bit e 64bit);
  Windows 11 (32bit e 64bit);
  CentOS 5 e 6 (32bit e 64bit);
  CentOS 7, 8 (64bit);
  Debian 7 ou superior (64bit);
  Ubuntu 16.04 ou superior;
  Amazon Linux 1 ou superior;
  CloudLinux 7 ou superior;
  AlmaLinux 8 ou superior;
- Processador:
  Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);
- Memória (RAM):
  Mínimo de 3GB exclusivamente para o agente da solução em desktops;
- Espaço de disco:
  Mínimo de 5GB.

Suporte Técnico

- O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;
- Horário de Atendimento: De segunda a sexta-feira, 8 horas por dia (entre 08:00hs e 17:00hs).

Serviços fora de escopo

- Instalação do agente

2.3.2.3. Serviço de Detecção e Resposta Estendida para Servidores;

Solução avançada de proteção para servidores fiscos, virtuais e em nuvem, integrada à plataforma de detecção e resposta estendida.

Este serviço contempla:

- 250 agentes de Endpoint Security (Pro);
- Proteção avançada baseada em machine learning (aprendizado de máquina - é um método de análise de dados que automatiza a construção de modelos analíticos);
- Identificação de ameaças baseada em análise comportamental;
- Detecção de ataques em memória;
- Antimalware de próxima geração;
- Bloqueio de ameaças via web reputation;
- Firewall de host (firewall em software que realiza o bloqueio de tráfego indesejado no dispositivo do usuário);
- Controle de aplicações;
- Monitoramento da integridade de arquivos, registros, bibliotecas e DLL do sistema operacional;
- Inspeção profunda dos logs do Sistema Operacional.;
- Identificação e blindagem de vulnerabilidades;
- Autoproteção do agente;
- Controle de dispositivos externos (USB, pen drive, HD externo);
- Endpoint detection and response – EDR (Detecção e Resposta de Endpoint);
- Integração nativa com a plataforma de detecção e resposta estendida

Atividades Previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;
- Administração centralizada da plataforma de detecção e resposta estendida:
- Atualização automática do software de segurança;
- Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas nas estações de trabalho e servidores;

- Auxílio para solucionar as ocorrências de vírus, malwares e exploits;
- Identificação de ameaças ou suspeita de contaminação do ambiente corporativo;
- Comunicação de incidências de vírus e de ameaças de computador desconhecidas.

Entregáveis

- Relatórios contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas, potenciais vulnerabilidades presentes em servidores;
- Relatório de TOP usuários, dispositivos e aplicações com risco;
- Relatório TOP hosts afetados por ameaças.

Pré-requisitos

- Sistema Operacional:
  Windows Server 2008 R2 (6.1);
  Windows Server 2012 (6.2);
  Windows Server 2012 R2 (6.3);
  Windows Server 2016 (10);
  Windows Server 2019;
  Linux RHEL 5, 6 (32bit e 64bit);
  Linux RHEL 7, 8, 9 (64bit);
  CentOS 5 e 6 (32bit e 64bit);
  CentOS 7, 8 (64bit);
  Debian 8 ou superior;
  Oracle Linux 5, 6 (32bit e 64bit);
  Oracle Linux 7 ou superior (64bit);
  Suse 12 ou superior;
  Ubuntu 16.04 ou superior;
  Amazon Linux 1 ou superior;
  CloudLinux 7 ou superior;
  AlmaLinux 8 ou superior.
- Processador:
  Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);
- Memória (RAM):
  Mínimo de 4.5GB.
- Espaço de disco:
  Mínimo de 5GB.

Suporte Técnico

- O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;
- Horário de Atendimento: De segunda a sexta-feira, 8 horas por dia (entre 08:00hs e 17:00hs).

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

Serviços fora de escopo

- Instalação do agente

2.3.2.4. Serviço de Proteção de Dados.

Este serviço contempla:

- Licenças para 3200 usuários de Zero Trust Secure Access - Private + Internet Access

Private Access

Solução para controle de acesso segmentado às aplicações corporativas, integrada à plataforma de detecção e resposta estendida, fundamentada na modelagem de risco cibernético e na metodologia Zero Trust. Contempla proteção robusta contra acessos não autorizados a aplicações internas.

Atividades Previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;
- Auxílio para solucionar as ocorrências de tentativas de acesso indevidos;
- Controle de acesso segmentando as aplicações internas;
- Análise comportamental de acessos e ataques direcionados aos usuários;
- Automatização para bloqueios de acessos indevidos a aplicações internas;
- Ações automatizadas de contenção de acessos indevidos;

Entregáveis

- Relatórios contemplando evidências do mapeamento de acessos monitorados a aplicações internas e ações de remediação executadas;
- Relatório de TOP usuários, dispositivos e aplicações com risco;

Pré-requisitos

- Sistema Operacional:
  Windows 10 (32bit e 64bit);
  Windows 11 (32bit e 64bit);
- Processador:
  Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);
- Memória (RAM):
  Mínimo de 3GB exclusivamente para o agente da solução em desktops;
- Espaço de disco:
  Mínimo de 5GB.
- Classificação mínima de informações críticas e/ou sensíveis.

Suporte Técnico

- O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;
- Horário de Atendimento: De segunda a sexta-feira, 8 horas por dia (entre 08:00hs e 17:00hs).

2.3.2.5. Internet Access

Solução para controle de acesso segmentado a internet, integrada à plataforma de detecção e resposta estendida, fundamentada na modelagem de risco cibernético e na metodologia Zero Trust. Contempla proteção robusta contra acessos não autorizados a sites externos.

Atividades Previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;
- Auxílio para solucionar as ocorrências de tentativas de acesso indevidos;
- Controle de acesso segmentando a internet;
- Análise comportamental de acessos e ataques direcionados aos usuários;
- Automatização para bloqueios de acessos indevidos a aplicações e sites;
- Ações automatizadas de contenção de acessos indevidos;

Entregáveis

- Relatórios contemplando evidências do mapeamento de acessos monitorados a aplicações internas e ações de remediação executadas;
- Relatório de TOP usuários, dispositivos e aplicações com risco;

Pré-requisitos

- Sistema Operacional:
  Windows 10 (32bit e 64bit);
  Windows 11 (32bit e 64bit);

Processador:

- Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);
- Memória (RAM):
- Mínimo de 3GB exclusivamente para o agente da solução em desktops;
- Espaço de disco:
- Mínimo de 5GB.
- Classificação mínima de informações críticas e/ou sensíveis.

Suporte Técnico

- O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;

2.3.3. Serviços de gestão e operação de segurança cibernética

Prestação de serviços especializados em segurança da informação, com foco na prevenção, detecção, resposta e recuperação de incidentes cibernéticos. A CONTRATADA será responsável por apoiar a CONTRATANTE na proteção de seus ativos de informação, garantindo a confidencialidade, integridade, disponibilidade e conformidade com normas e políticas internas e externas.

O serviço abrange desde a administração de soluções de segurança e firewalls até a análise de riscos, condução de treinamentos, resposta a incidentes, hardening, elaboração de relatórios e suporte técnico contínuo. A atuação será integrada às demais áreas de TI da CONTRATANTE, com foco em resiliência cibernética e melhoria contínua.

2.3.3.1. Atividades Previstas

- Suporte técnico e orientação em temas de segurança da informação;
- Administração, operação e implantação de soluções e equipamentos de segurança;
- Análise de riscos e elaboração de documentos de impacto aos negócios (BIA);
- Proposição e execução de melhorias no ambiente de segurança;
- Avaliação de segurança de aplicativos e infraestrutura;
- Identificação de riscos e impactos aos ativos da organização;
- Treinamentos e ações de conscientização em segurança da informação;
- Avaliação da segurança física e lógica, controle de mídias removíveis e realização de dois pentests anuais;
- Monitoramento de atividades relacionadas à segurança da informação.
- Coleta de evidências e elaboração de relatórios de incidentes;
- Garantia de conformidade com requisitos legais e regulatórios;
- Atuação em todas as fases de resposta a incidentes (preparação, detecção, contenção, erradicação e recuperação);
- Participação em reuniões técnicas e estratégicas;
- Implementação de ações de hardening e manutenção da base de conhecimento;
- Acompanhamento de fornecedores quando necessário.

2.3.3.2. Entregáveis

- Logs de restauração de backup;

- Relatório de análise de risco e impacto aos negócios (business impact analysis)
- Relatório de incidentes de segurança;
- Relatório de segurança cibernética contemplando as soluções de firewall e solução estendida contendo: Visão geral dos incidentes de segurança, discriminação dos tipos de incidentes com os detalhes técnicos dos incidentes detectados, top ameaças analisadas, top hosts infectados, recomendações de segurança, estatísticas do tráfego analisado, conexões VPN realizadas, bloqueios de tráfego malicioso detectados e prevenidos e indicadores de risco e vulnerabilidades do ambiente;
- Relatório de firewall de borda, VPN, IDS/IPS e filtro de Conteúdo;
- Relatório de solicitações;
- Relatório de ativos protegidos;
- Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade;
- Geração de Dashboards e exportação de dados para auditoria e conformidade (ISO 27001, NIST).;
- Relatório de detecção, priorização e acompanhamento de vulnerabilidades conforme MITRE ATT&CK com recomendações de segurança e tratamento;
- Relatório de incidentes e automações realizadas.

Obs.: Relatórios mediante alinhamento e definição de um modelo padrão

2.3.3.3. Este serviço é composto por:

✓ Analista de Proteção de Endpoints;
✓ Analista de Segurança de Perímetro em Redes/Firewall (Remoto);
✓ Governança como serviço sob demanda.

2.3.3.3.1. Analista de proteção de Endpoints

Contempla a gestão e suporte técnico especializado para as soluções previstas no escopo desta ESP relacionadas a Proteção de Tráfego de Rede, Detecção e Resposta Estendida para Estações de Trabalho e Servidores além do serviço de proteção de Dados. Certificações desejáveis.

Atividades previstas

- Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos a nível de endpoints, workloads e rede.
- Administração centralizada da plataforma de detecção e resposta estendidas:
- Atualização automática do software de segurança;
- Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas nas estações de trabalho e servidores;

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

- Auxílio para solucionar as ocorrências de vírus, malwares e exploits;
- Identificação de ameaças ou suspeita de contaminação do ambiente corporativo;
- Comunicação de incidências de vírus e de ameaças de computador desconhecidas.
- Monitoramento e notificação de alertas e comportamentos suspeitos a nível de rede;

Entregáveis

- Relatórios contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas, potenciais vulnerabilidades presentes em endpoints, workloads e rede.
- Relatório de TOP usuários, dispositivos e aplicações com risco;
- Relatório TOP hosts afetados por ameaças.

Obs.:Relatórios mediante alinhamento e definição de um modelo padrão.

Disponibilidade

- A disponibilidade do serviço especializado de gestão e suporte técnico é de 8 horas por dia (entre 08:00hs e 17:00hs), de segunda a sexta-feira.

2.3.3.3.2. Analista de Segurança de Perímetro em Redes/Firewall

A prestação dos serviços compreenderá a administração de equipamentos de segurança do tipo Firewall correspondentes ao atual parque (Vide Tabela de equipamentos do item VOLUMETRIA), executada por profissionais com certificações técnicas apenas desejáveis na área. O atendimento será realizado sob demanda, de forma remota, conforme a necessidade operacional identificada e o crescimento do parque de equipamentos.

A disponibilização dos recursos será realizada em conformidade com a disponibilidade contratual e respeitando os níveis de serviço acordados, assegurando a continuidade e a eficácia da proteção do ambiente de rede.

Atividades previstas

- Configuração: Configurar o firewall com as políticas de segurança adequadas, como regras de filtragem de pacotes, NAT (Network Address Translation), controle de acesso, mediante solicitação da CONTRATANTE;
- Atualização de Firmware e software: Manter o firewall atualizado com as últimas versões de firmware ou software para garantir as últimas correções de segurança e funcionalidades;
- Monitoramento: Monitorar o tráfego de rede que passa pelo firewall para identificar padrões incomuns, possíveis ataques ou violações de

políticas de segurança. Monitoramento constante da disponibilidade do firewall;

- Ajustes de regras: Ajustar as regras do firewall conforme necessário para garantir que esteja configurado para lidar com novos requisitos de rede, alterações de políticas de segurança ou novas ameaças;
- Gestão de Log: Gerenciar e analisar os logs de firewall para identificar atividades suspeitas, acompanhar o uso da largura de banda e manter registros para fins de conformidade e investigação de incidentes;
- Implementação de VPN: Configurar e gerenciar VPNs (Virtual Private Networks) para permitir conexões seguras entre redes remotas ou usuários remotos e a rede protegida pelo firewall;
- Backup: Realizar backups regulares das configurações do firewall e estabelecer procedimentos de recuperação para restaurar a configuração em caso de falha ou comprometimento;
- Administração Remota.

Entregáveis

- Relatório: Os relatórios serão emitidos conforme disponibilidade do produto apresentando consumo de CPU, memória, bloqueios.

Obs.:Relatórios mediante alinhamento e definição de um modelo padrão.

Serviços fora de escopo (Analista de Endpoint e de Segurança de Perímetro em Redes/Firewall):

- Infraestrutura e aplicação de informação da CPTM;
- Infraestrutura para integração com mainframe;
- Suporte à hardware (Reparo em servidores, switches e demais equipamentos de infraestrutura);
- Manutenção predial;
- Manutenção de infraestrutura de salas técnicas (Ar condicionado, rede/circuitos elétricos, no-breaks, geradores, etc);
- Operação, suporte e manutenção de:
- Sistemas de informação hospedados no ambiente;
- Solução CFTV (Hardware e Software);
- Solução de videowall (Hardware e Software);
- Catracas;
- Cancelas;
- PABX TDM (telefonia em geral).
- Fornecimento de ferramentas, equipamentos, materiais e softwares, exceto computadores para os profissionais alocados com o pacote MS Office;
- Soluções de proteção antivírus para e-mails (tanto internos à organização do cliente quanto externos, pelo protocolo SMTP), mesmo

que trafeguem na rede e nas estações de trabalho, incluindo licenças, gerenciamento e qualquer ação a respeito da solução;
- Instalação do agente nas estações de trabalho;
- Elaboração e definição de políticas relacionadas à segurança da informação;
- Fornecimento ou substituição de hardware e software;
- Identificação de ameaças e vulnerabilidades em dispositivos que não possuem um agente (Endpoint, Workload e ZTSA) instalado.
- Testes de intrusão em serviços e aplicações;
- Suporte a soluções de firewall de código aberto (open source);
- Serviços de suporte aos desktops e usuários (service desk);
- Desenvolvimento e manutenção de aplicativos e sistemas;
- Fornecimento de licenças de software em geral, exceto aqueles já contemplados nos serviços contratados;
- Migração de dados nos casos de troca ou substituição de máquina;
- Suporte para utilização e reparos de software;
- Infraestrutura em geral;
- Gerenciamento, monitoramento, manutenção e suporte à infraestrutura em geral e aos usuários no ambiente de TIC;
- Manutenção de hardwares e ativos do cliente;
- Intervenções estruturais (paredes, telhados, teto, forros, instalações elétricas, cabeamento de rede), ou áreas de periculosidade;
- Implantação e administração de ambientes de BI (business intelligence);
- Quaisquer outras atividades não explicitadas neste RPT;
- Administração da plataforma Lotus Notes;
- Operação, suporte, administração de sistemas de informações hospedados no ambiente.

Disponibilidade

- Atuação da equipe será no horário das 07h às 19h de segunda a sexta feira de forma remota.
- O suporte de cada serviço fora do expediente regular deverá ser prestado em regime de sobreaviso e plantões, no qual um dos profissionais da equipe permanecerá disponível para atendimentos remotos, quando acionado de segunda a sexta-feira, nos horários não cobertos pelo expediente comercial, e também aos sábados, domingos e feriados.

2.3.3.3.3. Governança

Apoio para atualização de políticas

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

Atividades previstas

- Elaboração e manutenção de políticas, normas e procedimentos;
- Validação de controles de compliance (LGPD, ISO 27001, regulatórios etc.);
- Sensibilização para conscientização em segurança da informação;

Entregáveis

- Políticas, normas e procedimentos atualizados de segurança da informação;
- Programas de conscientização;

Serviços fora de escopo

- Suporte Técnico Operacional (N1/N2/N3);
- Infraestrutura de TI;
- Execução técnica de soluções;
- Projetos ou entregas fora do planejamento da governança;
- Serviços não relacionados à segurança da informação.

Disponibilidade

- Sob demanda como serviços e não alocação de recursos.

2.3.3.4. NÍVEIS DE SERVIÇOS

2.3.3.4.1. Indicadores e Entregáveis

Serviço	Indicador de Desempenho (KPI)	Métrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
Gestão e operação de segurança cibernética	Início de atendimento para incidentes de segurança	< 2 horas	Mensal	Penalidade de 1% no pagamento mensal do serviço por incidente	Relatório de incidentes de segurança
	Relatório de gestão de segurança	95% dos eventos registrados e apresentados	Mensal	Penalidade de 3% no pagamento mensal do serviço	Relatório de segurança cibernética contemplando as soluções de firewall e solução estendida contendo: Visão geral dos incidentes de segurança, discriminação dos tipos de incidentes com os detalhes técnicos dos incidentes detectados, top ameaças analisadas, top hosts infectados, recomendações de segurança, estatísticas do tráfego analisado, conexões VPN realizadas, bloqueios de tráfego malicioso detectados e prevenidos e indicadores de risco e vulnerabilidades do ambiente.

2.3.3.4.2. Indicadores e Entregáveis

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
Solução de Firewall	Disponibilidade da Plataforma de Firewall fornecida como serviço	99%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de firewall de borda, VPN, IDS/IPS e filtro de Conteúdo
	Disponibilidade da plataforma firewall existente no contratado	99%	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de firewall de borda, VPN, IDS/IPS e filtro de Conteúdo
	Gestão de regras e políticas de segurança	até 8 horas úteis	Mensal	Penalidade de 1% no pagamento mensal do serviço	Relatório de solicitações

2.3.3.4.3. Indicadores e Entregáveis

Serviço	Indicador de Desempenho (KPI)	Metrica	Frequência de Medição	Penalidade por Não Conformidade	Relatórios e Entregáveis
Solução estendida de detecção e resposta, segurança de endpoints e rede	Antivírus para estações de trabalho no domínio	95% do parque protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos
	Antivírus para servidores	99% do parque protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos
	Ativos fora da rede	80% protegido e atualizado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de ativos protegidos
	Identificação e correlação automática de eventos suspeitos em múltiplos vetores (endpoints, rede, servidores, cloud, firewall)	95% identificado e correlacionado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade
	Análise automática do tráfego e detecção de comportamentos anômalos	95% analisado e tratado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade
	Relatórios de conformidade	95% sob demanda	Mensal	Penalidade de 1% no pagamento mensal do serviço	Geração de Dashboards e exportação de dados para auditoria e conformidade (ISO 27001, NIST)
	Detecção baseada em IA de desvios comportamentais de usuários e dispositivos	95% analisado e tratado	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório semanal contendo as ameaças detectadas, tratadas e classificadas por criticidade
	Relatório de Vulnerabilidades	90% das vulnerabilidades identificadas	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de detecção, priorização e acompanhamento de vulnerabilidades conforme MITRE ATT&CK com recomendações de segurança e tratamento.
	Execução de playbooks de resposta automática a incidentes	95% de eficácia nas regras de automação configuradas	Mensal	Penalidade de 5% no pagamento mensal do serviço	Relatório de incidentes e automações realizadas

2.3.3.5. VOLUMETRIA

Para efeito de dimensionamento para prestação dos serviços e atendimentos aos níveis de serviços acordados, o parque de equipamentos e usuários de informática da CONTRATADA estão distribuídos, conforme quadro abaixo:

TIPO	QUANTIDADE
Usuários	6000
Desktops	2653
Thin Client	109
Notebooks	398
Servidores físicos	20
Servidores virtuais	193 (229)
Tablets	107
Switches	602
Roteadores	226
Firewalls	06
Links Intragov	212
Racks	315
Storage (TB)	605
Chamados SD	2925/mês

3. PRAZOS

O cronograma para a execução dos trabalhos previstos nesta ESP será estabelecido de comum acordo entre as partes.

4. RESPONSABILIDADE DAS PARTES

Além das obrigações constantes da Cláusula "**OBRIGAÇÕES DAS PARTES**" do Contrato a que se vincula esta ESP ficam definidas as enunciadas a seguir:

4.1. DA CONTRATADA

4.1.1. Designar as pessoas responsáveis que serão os interlocutores autorizados para o relacionamento com a CONTRATANTE;

4.1.2. Comunicar com antecedência mínima de 24 horas, todas as manutenções e/ou intervenções rotineiras no Data Center Prodesp que possam significar paralisações dos servidores ou dos serviços prestados;

4.1.3. Comunicar imediatamente, todas as ocorrências imprevistas que prejudiquem a prestação de serviços;

4.2. DA CONTRATANTE

4.2.1. Designar as pessoas responsáveis que serão os interlocutores autorizados para o relacionamento com a CONTRATADA;

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

4.2.2. Assegurar a participação da CONTRATADA em quaisquer projetos que possam afetar os serviços definidos;

4.2.3. Assumir integralmente, sem solidariedade da CONTRATADA, seja a que título for a responsabilidade pela utilização do Usuário e Senha;

4.2.4. Observar rigorosamente as instruções e procedimentos fornecidos pela CONTRATADA;

4.2.5. Manter a suas expensas Link Intragov ou acesso à Internet;

4.2.6. Assegurar a participação da CONTRATADA em quaisquer projetos que possam afetar os serviços definidos;

4.2.7. A utilização de nomes de usuários e senhas, os serviços que prestar e conteúdo que trafegar a partir dos recursos e serviços objeto desta ESP.

5. PREÇO E CONDIÇÕES DE PAGAMENTO

O preço para a execução dos serviços constantes desta Especificação de Serviços e Preços é estimado em **R$ 54.822.367,80 (cinquenta e quatro milhões, oitocentos e vinte e dois mil, trezentos e sessenta e sete reais e oitenta centavos)**, tendo como data base de referência o mês de **julho/2025** e será reajustado de acordo com as condições estabelecidas no contrato a que se vincula.

ITEM	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	QTDE		VALOR UNITÁRIO	QTDE MESES	PARCELA MENSAL	TOTAL
			MÊS	TOTAL				
5.1	**Solução de Gestão do Ambiente de TI**	**POR MÊS**	**1**	**30**	**R$ 7.611,07**	**30**	**R$ 7.611,07**	**R$ 228.332,10**
5.2	**Serviço Técnicos Especializados em TI**						**R$ 1.025.246,73**	**R$ 30.757.401,90**
5.2.1	Serviço de coordenação de operação de TI e Projetos	POR MÊS	1	30	R$ 229.007,98	30	R$ 229.007,98	R$ 6.870.239,40
5.2.2	Serviço de monitoramento de ambiente de TI - NOC	POR MÊS	1	30	R$ 99.375,96	30	R$ 99.375,96	R$ 2.981.278,80
5.2.3	Serviço de gestão e operação do ambiente de rede Corporativa	POR MÊS	1	30	R$ 95.020,81	30	R$ 95.020,81	R$ 2.850.624,30
5.2.4	Serviço de administração e operação de Banco de Dados	POR MÊS	1	30	R$ 200.705,90	30	R$ 200.705,90	R$ 6.021.177,00
5.2.5	Serviço de gestão e operação do ambiente virtualizado	POR MÊS	1	30	R$ 264.695,00	30	R$ 264.695,00	R$ 7.940.850,00
5.2.6	Serviço de gestão e operação de soluções de armazenamento	POR MÊS	1	30	R$ 92.670,54	30	R$ 92.670,54	R$ 2.780.116,20
5.2.7	Serviço de gestão e operação de backup	POR MÊS	1	30	R$ 43.770,54	30	R$ 43.770,54	R$ 1.313.116,20
5.3	**Serviço de Segurança com Tratamento e Resposta à Incidentes Cibernéticos**						**R$ 794.554,46**	**R$ 23.836.633,80**
5.3.1	Solução de firewall	POR MÊS	1	30	R$ 146.541,48	30	R$ 146.541,48	R$ 4.396.244,40
5.3.2	Solução estendida de detecção e resposta, segurança de endpoints e rede	POR MÊS	1	30	R$ 415.303,75	30	R$ 415.303,75	R$ 12.459.112,50
5.3.3	Serviços de gestão e operação de segurança cibernética	POR MÊS	1	30	R$ 232.709,23	30	R$ 232.709,23	R$ 6.981.276,90
TOTAL							**R$ 1.827.412,26**	**R$ 54.822.367,80**

Os subitens serão faturados em parcela fixa mensais.

Serão emitidas Notas Fiscais Eletrônicas e enviadas, automaticamente, pelo sistema das Prefeituras (Taboão da Serra e São Paulo), sendo que para os serviços prestados em Taboão da Serra, serão encaminhadas para o e-mail

cadastrado no sistema de contratos da Prodesp, e para os serviços prestados em São Paulo, para o e-mail cadastrado junto àquela Prefeitura.

Recebidas as Notas-Fiscais Eletrônicas, a CONTRATANTE terá o prazo de 03 (três) dias para atestação da execução dos serviços ou devolução para esclarecimentos e correções necessárias.

Os pagamentos deverão ser efetuados dentro do prazo de 30 (trinta) dias da data de apresentação das Notas-Fiscais Eletrônicas.

6. VIGÊNCIA DO DOCUMENTO

A ESP terá vigência de **30 (trinta)** meses a partir da data da assinatura do Contrato.

7. VALIDADE DOS PREÇOS

Os preços constantes desta ESP são válidos por **120 (cento e vinte)** dias após a data de sua emissão.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

8. CONTATO NA PRODESP

Os contatos relativos ao objeto constante desta ESP deverão ser feitos com:

ÁREA DE NEGÓCIOS

Nome : Bruno Baranda
Endereço: Rua Agueda Gonçalves, 240 - 2º andar - Taboão da Serra - SP
Telefone : (11) 2868-3124
E-mail : bruno.baranda@sp.gov.br

ÁREA RESPONSÁVEL PELA EXECUÇÃO DO SERVIÇO

Nome : Luciano Benato
Endereço: Rua Agueda Gonçalves, 240 - Taboão da Serra - SP.
Telefone : (11) 2845-6000
E-mail : benato@sp.gov.br

Nome : Rodrigo Gomes de Moura
Endereço : Rua Agueda Gonçalves, 240 - Taboão da Serra - SP.
Telefone : (11) 2845-6468
E-mail : rgmoura@sp.gov.br

Nome : Jobson Nunes de Souza
Endereço : Rua Agueda Gonçalves, 240 - Taboão da Serra - SP.
Telefone : (11) 2845-6344
E-mail : jobson.souza@sp.gov.br

De acordo

CONTRATANTE

Nome:
Cargo:

Emissão: 24/07/2025

ANEXO I
PLANILHA DE ORÇAMENTO
ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS E0240557
CONTRATO PD024401
COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM

ITEM	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	QTDE		VALOR UNITÁRIO	QTDE MESES	PARCELA MENSAL	TOTAL
			MÊS	TOTAL				
5.1	**Solução de Gestão do Ambiente de TI**	**POR MÊS**	**1**	**30**	**R$ 7.611,07**	**30**	**R$ 7.611,07**	**R$ 228.332,10**
5.2	**Serviço Técnicos Especializados em TI**						**R$ 1.025.246,73**	**R$ 30.757.401,90**
5.2.1	Serviço de coordenação de operação de TI e Projetos	POR MÊS	1	30	R$ 229.007,98	30	R$ 229.007,98	R$ 6.870.239,40
5.2.2	Serviço de monitoramento de ambiente de TI - NOC	POR MÊS	1	30	R$ 99.375,96	30	R$ 99.375,96	R$ 2.981.278,80
5.2.3	Serviço de gestão e operação do ambiente de rede Corporativa	POR MÊS	1	30	R$ 95.020,81	30	R$ 95.020,81	R$ 2.850.624,30
5.2.4	Serviço de administração e operação de Banco de Dados	POR MÊS	1	30	R$ 200.705,90	30	R$ 200.705,90	R$ 6.021.177,00
5.2.5	Serviço de gestão e operação do ambiente virtualizado	POR MÊS	1	30	R$ 264.695,00	30	R$ 264.695,00	R$ 7.940.850,00
5.2.6	Serviço de gestão e operação de soluções de armazenamento	POR MÊS	1	30	R$ 92.670,54	30	R$ 92.670,54	R$ 2.780.116,20
5.2.7	Serviço de gestão e operação de backup	POR MÊS	1	30	R$ 43.770,54	30	R$ 43.770,54	R$ 1.313.116,20
5.3	**Serviço de Segurança com Tratamento e Resposta à Incidentes Cibernéticos**						**R$ 794.554,46**	**R$ 23.836.633,80**
5.3.1	Solução de firewall	POR MÊS	1	30	R$ 146.541,48	30	R$ 146.541,48	R$ 4.396.244,40
5.3.2	Solução estendida de detecção e resposta, segurança de endpoints e rede	POR MÊS	1	30	R$ 415.303,75	30	R$ 415.303,75	R$ 12.459.112,50
5.3.3	Serviços de gestão e operação de segurança cibernética	POR MÊS	1	30	R$ 232.709,23	30	R$ 232.709,23	R$ 6.981.276,90
TOTAL							**R$ 1.827.412,26**	**R$ 54.822.367,80**

ANEXO 3

CONTRATO CPTM DL00925-01 / PRODESP PD024401

CRONOGRAMA FÍSICO FINANCEIRO

CPTM

CRONOGRAMA FÍSICO X FINANCEIRO

Mês	Parcela Mensal	
1	R$	1.827.412,26
2	R$	1.827.412,26
3	R$	1.827.412,26
4	R$	1.827.412,26
5	R$	1.827.412,26
6	R$	1.827.412,26
7	R$	1.827.412,26
8	R$	1.827.412,26
9	R$	1.827.412,26
10	R$	1.827.412,26
11	R$	1.827.412,26
12	R$	1.827.412,26
13	R$	1.827.412,26
14	R$	1.827.412,26
15	R$	1.827.412,26
16	R$	1.827.412,26
17	R$	1.827.412,26
18	R$	1.827.412,26
19	R$	1.827.412,26
20	R$	1.827.412,26
21	R$	1.827.412,26
22	R$	1.827.412,26
23	R$	1.827.412,26
24	R$	1.827.412,26
25	R$	1.827.412,26
26	R$	1.827.412,26
27	R$	1.827.412,26
28	R$	1.827.412,26
29	R$	1.827.412,26
30	R$	1.827.412,26
Total	R$	54.822.367,80

Governo do Estado de São Paulo
Companhia Paulista de Trens Metropolitanos
Depto De Contratacoes E Compras

Contrato

ANEXO 4

CONTRATO DL00925-01 / PRODESP PD024401

DECLARAÇÃO DE CIÊNCIA E RESPONSABILIDADE

Pelo presente, nós, GILENO GURJÃO BARRETO e THIAGO WALTZ ALVES, representantes da COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP ("Empresa"), inscrita sob nº. 62.577.929/0001-35, na qualidade de Fornecedor, ou Prestador de Serviço, ou Parceiro da CPTM, neste ato declaramos estarmos cientes dos termos do Código de Conduta e Integridade de Fornecedores, Prestadores de Serviços e Parceiros da CPTM, comprometendo-nos a adotar as práticas indicadas nele para a realização das atividades nossas e da Empresa, bem como manter a confidencialidade de todas e quaisquer informações recebidas para o desenvolvimento das atividades relativas à CPTM, mesmo depois do término da relação contratual entre a CPTM e a Empresa.

Além disso, com relação às questões de corrupção, declaramos que nós e a Empresa estamos de acordo com as diretrizes apresentadas neste Código, acessado através do endereço eletrônico https://www.cptm.sp.gov.br/cptm/esg-consciente/praticas-de-governanca/codigos-de-conduta-integridade, e entendemos que estamos proibidos de oferecer, prometer, pagar, autorizar ou receber quaisquer pagamentos indevidos, bem como realizar fraudes de qualquer natureza.

Declaramos ainda que a Empresa cumpre as Leis Aplicáveis de combate à Corrupção e que disseminamos e esperamos a mesma conduta de nossos funcionários, fornecedores, parceiros comerciais, funcionários terceirizados e representantes.

GILENO GURJÃO BARRETO
Diretor Presidente
gileno.barreto@sp.gov.br
e-mail pessoal: N/I
CPF nº 315.099.595-72
RG nº 842.620 SSP-SE

THIAGO WALTZ ALVES
Diretor Comercial
thiago.waltz@sp.gov.br
e-mail pessoal: N/I
CPF nº 950.082.761-15
RG nº 1.855.322 SSP-DF

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 12/11/2025, às 18:35, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0088904949** e o código CRC **92213106**.

Contrato

ANEXO 5

CONTRATO DL00925-01 / PRODESP PD024401

TERMO DE CONFIDENCIALIDADE E USO

A CONTRATADA COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP, inscrita no CNPJ sob o número 62.577.929/0001-35, com sede em Taboão da Serra/SP, na Rua Agueda Gonçalves nº 240 – Jd. Pedro Gonçalves, doravante designada Signatário, neste ato representada por GILENO GURJÃO BARRETO, inscrito(a) no CPF sob o número 315.099.595-72 , e THIAGO WALTZ ALVES, inscrito(a) no CPF sob o número 950.082.761-15 aceita as regras, condições e obrigações constantes do presente Termo.

1. O objeto deste Termo de Confidencialidade e Uso é prover a necessária e adequada proteção às Informações Restritas, de propriedade exclusiva e/ou sob controle da Contratante, reveladas ao Signatário ou por ele acessíveis, em função da execução do objeto do contrato DL00925-01 / PRODESP PD024401.

2. A expressão “Informações Restritas” abrange toda informação escrita, oral ou de qualquer modo apresentada, tangível ou intangível, pessoal ou não, incluídas, mas não se limitando, a manifestações técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, planos de negócios e processos.

3. O Signatário compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da Contratante, das informações restritas a ele reveladas ou por ele acessadas.

4. O Signatário compromete-se a não utilizar, de forma diversa da prevista no contrato celebrado com a Contratante, as informações restritas a ele reveladas ou por ele acessadas.

5. O Signatário deverá cuidar para que as informações a ele reveladas ou por ele acessadas, fiquem limitadas ao seu próprio conhecimento.

6. O Signatário obriga-se a informar imediatamente à Contratante, qualquer violação das regras de confidencialidade e uso estabelecidas neste Termo de que tenha tomado conhecimento ou que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

7. A quebra de confidencialidade ou das condições de uso das Informações Restritas reveladas ou acessadas, por ação ou omissão de Signatário, devidamente comprovada, sem autorização expressa da Contratante, sujeitará o Signatário às consequências legais e sanções cabíveis, ao pagamento ou recomposição de todas as perdas e danos sofridos pela Contratante, inclusive os de ordem moral, bem como às responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial e administrativo.

8. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às Informações Restritas de propriedade exclusiva e/ou sob controle da Contratante.

9. O Signatário manifesta explícita ciência e se compromete a observar as normas de segurança, privacidade e proteção de dados.

10. O Signatário deve assegurar que as obrigações assumidas por meio do presente instrumento sejam conhecidas e cumpridas por seus empregados, prepostos e/ou colaboradores internos/externos.

E, por aceitar todas as condições e obrigações constantes do presente Termo, o Signatário assina o presente Termo.

GILENO GURJÃO BARRETO
Diretor Presidente
gileno.barreto@sp.gov.br
e-mail pessoal: N/I
CPF nº 315.099.595-72
RG nº 842.620 SSP-SE

THIAGO WALTZ ALVES
Diretor Comercial
thiago.waltz@sp.gov.br
e-mail pessoal: N/I
CPF nº 950.082.761-15
RG nº 1.855.322 SSP-DF

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 12/11/2025, às 16:31, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 12/11/2025, às 18:35, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0088905090** e o código CRC **11209033**.

Governo do Estado de São Paulo
Companhia Paulista de Trens Metropolitanos
Depto De Contratacoes E Compras

Contrato

ANEXO 6

CONTRATO DL00925-01 / PRODESP PD024401

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM
CONTRATADA: COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP
CONTRATO: DL00925-01 / PRODESP PD024401
OBJETO: PRESTAÇÃO DE SERVIÇOS CONTINUADOS, ESPECIALIZADOS EM TI – TECNOLOGIA DA INFORMAÇÃO, QUE SE CONSTITUEM DE UMA SOLUÇÃO GLOBAL AO AMBIENTE DE TI E DE SEGURANÇA CIBERNÉTICA.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial Eletrônico do Tribunal de Contas do Estado de São Paulo (https://doe.tce.sp.gov.br/), em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante e interessados estão cadastradas no módulo eletrônico do “Cadastro Corporativo TCESP – CadTCESP”, nos termos previstos no Artigo 2º das Instruções nº01/2024, conforme “Declaração(ões) de Atualização Cadastral” anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

LOCAL: São Paulo/SP

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome: MICHAEL SOTELO CERQUEIRA
Cargo: Diretor Presidente
CPF: 284.295.458-08

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:

Nome: MICHAEL SOTELO CERQUEIRA
Cargo: Diretor Presidente
CPF: 284.295.458-08

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:
Pelo contratante:
Nome: ANA CAROLINE DE FARIA EDUARDO BORGES
Cargo: Diretora Administrativa e Financeira
CPF: 003.938.371-73

Nome: MICHAEL SOTELO CERQUEIRA
Cargo: Diretor Presidente
CPF: 284.295.458-08

Nome: GEAN LIMA FERREIRA
Cargo: Gerente de Tecnologia da Informação
CPF: 270.806.028-74

Pela contratada:
Nome: GILENO GURJÃO BARRETO
Cargo: Diretor Presidente
CPF: 315.099.595-72

Nome: THIAGO WALTZ ALVES
Cargo: Diretor Comercial
CPF: 950.082.761-15

ORDENADOR DE DESPESAS DA CONTRATANTE:
Nome: MICHAEL SOTELO CERQUEIRA
Cargo: Diretor Presidente
CPF: 284.295.458-08

Gestor do contrato:
Nome: LEONARDO MARQUES LOPES
Cargo: Chefe do Departamento de Operação de TI
CPF: 377.303.338-99

Documento assinado eletronicamente por **Leonardo Marques Lopes**, **Chefe De Departamento**, em 11/11/2025, às 14:34, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gean Lima Ferreira**, **Gerente**, em 11/11/2025, às 14:36, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Michael Sotelo Cerqueira**, **Diretor Presidente**, em 11/11/2025, às 18:52, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 12/11/2025, às 16:31, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 12/11/2025, às 18:35, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Ana Caroline De Faria Eduardo Borges**, **Diretor**, em 13/11/2025, às 09:18, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0088905232** e o código CRC **E1BE64E1**.