CONTRATAÇÃO DE SERVIÇOS NECESSÁRIOS PARA A IMPLANTAÇÃO, FUNCIONAMENTO E MANUTENÇÃO DE UM *SECURITY OPERATIONS CENTER* (SOC) PELO PRAZO MÍNIMO DE 36 MESES. O SOC SERÁ COMPOSTO POR: SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA (*BLUE TEAM*); SERVIÇO DE GESTÃO TESTES DE INVASÃO (*RED TEAM*) E SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO, SOB REGIME DE EMPREITADA POR PREÇO UNITÁRIO, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ E A EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA. (PROCESSO ADMINISTRATIVO N. 8521639-33.2023.8.06.0000).

CT N. 15/2024
CÓDIGO DA CONTRATAÇÃO (PAC): TJCESETIN_UGP_2023_09

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**, situado no Centro Administrativo Governador Virgílio Távora, com sede na Avenida General Afonso Albuquerque Lima, S/N, Bairro Cambeba, Fortaleza – CE, inscrito no CNPJ sob o número 09.444.530/0001-01, doravante denominado simplesmente de **TJCE** ou CONTRATANTE, neste ato representado por seu Presidente, Des. Antônio Abelardo Benevides Moraes e por sua Secretária de Tecnologia da Informação, Denise Maria Norões Olsen, e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, representada neste ato por Yure Leopoldo Sabino de Freitas, portador da carteira de identidade sob o nº. 559056187 - Expedida por: SPP-SP, CPF n. 525.285.023-20, com endereço na Av. Pontes Vieira, nº 2340, Dionísio Torres, UNO – Medical & Office – Sala 510 – 514, 5º andar, em Fortaleza/CE, inscrita no CNPJ sob o número 05.250.796/0001-54, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei n. 14.133, de 21 de abril de 2021 e pela Resolução n. 169, de 31 de janeiro de 2013, do Conselho Nacional de Justiça, com suas alterações e atualizações posteriores.

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da licitação realizada sob a modalidade Pregão Eletrônico n. 019/2023, devidamente homologada pelo Exmo. Desembargador Presidente do Tribunal de Justiça do Estado do Ceará, tudo em conformidade com as disposições da Lei Nacional n. 14.133/2021, com suas alterações e atualizações posteriores, e o processo administrativo n. 8521639-33.2023.8.06.0000.

PARÁGRAFO ÚNICO – REGIME DE CONTRATAÇÃO

A execução da presente avença será **indireta**, segundo o regime de execução por **preço unitário**, nos termos dos art. 6°, XXVIII da Lei n. 14.133/21, sendo originário da licitação na modalidade de Pregão, na forma eletrônica, sob o número 019/2023.

CLÁUSULA SEGUNDA – DO OBJETO

O objeto deste Instrumento consiste na ***Contratação de serviços necessários para a implantação, funcionamento e manutenção de um Security Operations Center (SOC) pelo prazo mínimo de 36 meses. O SOC será composto por: Serviço de gestão de incidentes de segurança (Blue Team); Serviço de gestão testes de invasão (Red Team) e Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação***, pelo regime de execução indireta, conforme especificações contidas no Edital do Pregão Eletrônico n. 019/2023 e seus anexos, bem como nos Anexos deste Contrato, todos, partes do mesmo.

§ 1º DOCUMENTAÇÃO COMPLEMENTAR

Os documentos constantes do Processo Administrativo nº **8521639-33.2023.8.06.0000** integram o presente Termo de Contrato como se nele estivessem transcritos, cujos teores consideram-se conhecidos e acatados pelas partes, sem prejuízos da aplicação de normas técnicas e legislação vigentes relativas ao objeto contratual, especialmente quanto a(ao):

a. Termo de Referência;
b. Edital e demais anexos do Edital de Pregão Eletrônico nº 019/2023; e,
c. Proposta da CONTRATADA, no que couber.

§ 2º A prestação dos serviços obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Contrato, no que não o contrarie.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DAS PARTES

São obrigações das partes neste Termo de Contrato:

§1° **DO CONTRATANTE**

I. Designar formalmente, na forma do art. 177, da Lei nº 14.133/21, representantes para gerenciar e exercer a fiscalização da execução do Contrato, independentemente do acompanhamento e controle exercido pela CONTRATADA.

II. Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste contrato, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE.

III. Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. Ele deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

IV. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas.

V. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com os termos do contrato assinado.

VI. Proporcionar todas as condições e prestar as informações necessárias para que a CONTRATADA possa cumprir com suas obrigações, dentro das normas e condições contratuais.

VII. Prestar, por meio do Fiscal Técnico do Contrato, as informações e os esclarecimentos pertinentes aos serviços/bens avençados, que porventura venham a ser solicitados pela

CONTRATADA.

VIII. Informar à CONTRATADA sobre atos que possam interferir direta ou indiretamente nos serviços prestados/entrega de bens.

IX. Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

X. Registrar e oficializar a CONTRATADA sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

XI. Rejeitar, no todo ou em parte, os serviços executados que não atendam às especificações técnicas deste Termo de Contrato.

XII. Aprovar ou rejeitar, no todo ou em parte, os serviços executados ou entrega de equipamentos, que não estiverem em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

XIII. Efetuar o pagamento devido pela prestação dos serviços executados, desde que cumpridas todas as formalidades e exigências avençadas.

XIV. Aplicar as sanções previstas em contrato, assegurando à CONTRATADA o contraditório e a ampla defesa.

XV. Exigir, sempre que necessário, a apresentação da documentação pela CONTRATADA que comprove a manutenção das condições que ensejaram a sua contratação.

§2° **DA CONTRATADA**

I. Manter atualizados seus dados cadastrais junto ao TJCE.

II. Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela CONTRATADA, sem ônus adicional ao TJCE.

III. Cumprir fielmente os Níveis Mínimos de Serviço (NMS), conforme o **item 5 do ANEXO I – Serviços Gerenciados de Segurança da Informação**, e demais especificações técnicas deste Termo de Contrato.

IV. Conceder acesso ao TJCE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do TJCE.

V. Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJCE, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.

VI. Credenciar devidamente um Preposto para representá-lo em todas as questões relativas ao cumprimento dos serviços, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa com o TJCE e a equipe da CONTRATADA, sem custo adicional.

VII. Assumir total responsabilidade pela execução dos serviços, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.

VIII. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Contrato, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.

IX. Comunicar ao TJCE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos.

X. Submeter ao TJCE qualquer alteração que se tornar essencial à continuação da execução dos serviços.

XI. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

XII. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.

XIII. Selecionar e preparar rigorosamente o(s) empregado(s) que irá(ão) prestar os serviços.

XIV. Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência.

XV. Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços.

XVI. Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, realizando-os de forma meticulosa e constante, mantendo sempre em perfeita ordem.

XVII. Orientar seus empregados de que não poderão se retirar dos prédios ou instalações do CONTRATANTE portando volumes ou objetos sem a devida autorização e liberação do Fiscal do contrato.

XVIII. Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do CONTRATANTE, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

XIX. Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento.

XX. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço ou entrega de bens, ou em conexão com ele, ainda que acontecido em dependências do CONTRATANTE.

XXI. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.

XXII. Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços ou entrega de bens, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente.

XXIII. Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.

XXIV. Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua regularização.

XXV. Não transferir a outrem, no todo ou em parte, a execução do contrato.

XXVI. Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

XXVII. Responsabilizar-se pela conduta do empregado que for incompatível com as normas do CONTRATANTE, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação.

XXVIII. Receber as observações do Fiscal Técnico do contrato, relativamente ao desempenho das atividades/entrega de bens, e identificar as necessidades de melhoria.

XXIX. Registrar e controlar, diariamente, as ocorrências e os serviços sob sua responsabilidade.

XXX. Permitir a fiscalização e o acompanhamento da execução do objeto deste Termo de

Contrato por servidor designado pelo CONTRATANTE, em conformidade com o artigo 117 da Lei nº 14.133/21.

XXXI. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21.

XXXII. Indenizar quaisquer danos ou prejuízos causados ao TJCE ou a terceiros, por ação ou omissão do seu pessoal durante a execução dos serviços/entrega de bens.

XXXIII. Não colocar à disposição do CONTRATANTE, para o exercício de funções de chefia, pessoal que incidam na vedação dos artigos 1º e 2º da Resolução nº 156/2012 do Conselho Nacional de Justiça (Art. 4º – Resolução 156/2012 – CNJ).

XXXIV. Encaminhar para o atesto dos fiscais, as faturas emitidas dos serviços prestados.

XXXV. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o CONTRATANTE for compelido a responder em decorrência desta avença.

XXXVI. Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços ou entrega de bens, da relação contratual mantida com o CONTRATANTE.

XXXVII. Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

XXXVIII. Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.

XXXIX. Comprovar vínculo empregatício dos profissionais disponibilizados para prestação dos serviços objeto desta contratação através de Ficha de Registro de Empregado, ou Carteira de Trabalho, ou contrato de prestação de serviço (ou documento similar) ou ainda Contrato Social da empresa, em casos de vínculo societário.

XL. Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Contrato por servidor designado pelo contratante.

XLI. Não subcontratar, ceder ou transferir, total ou parcial o objeto desta contratação.

XLII. Recrutar e selecionar os profissionais necessários à realização do serviço, de acordo com a qualificação técnica exigida, a ser previamente submetida ao Fiscal para verificação da conformidade.

XLIII. Fornecer ao TJCE, ao início da prestação do serviço, a relação nominal dos técnicos que atuarão no cumprimento do objeto contratado, atualizando-a sempre que necessário.

XLIV. Tal documentação deverá ser juntada nos autos dos contratos.

XLV. Manter atualizada a documentação comprobatória da qualificação dos profissionais alocados na execução do serviço e disponibilizar essa documentação ao Tribunal, sempre que solicitada.

XLVI. Manter o TJCE formalmente avisado sobre demissões de profissionais que prestem serviço nas dependências do Tribunal, para fins de cancelamento da autorização de entrada e acessos a recursos, sistemas e aplicativos do TJCE.

XLVII. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos, níveis, indicadores e condições não sejam cumpridos.

XLVIII. Conceder acesso ao TJCE, o controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do mesmo.

CLÁUSULA QUARTA – DA DESCRIÇÃO DA SOLUÇÃO E DAS ESPECIFICAÇÕES TÉCNICAS

A CONTRATANTE atenderá às especificações e às condições de execução dos serviços, nos termos definidos nesta cláusula.

§1° DESCRIÇÃO DA SOLUÇÃO

I. Fornecimento de serviços para a implantação de um *Security Operations Center* (SOC), que é uma unidade imprescindível para a segurança da informação do TJCE, composta por diferentes equipes especializadas. Nesta contratação de serviços, as soluções requeridas são:

a) Serviço de gestão de incidentes de segurança (*Blue Team*): Serviço de desenvolvimento, planejamento, acompanhamento de implantação e manutenção das medidas de segurança da informação do TJCE, bem como detectar incidentes e elaborar estratégias, diagnosticar e acompanhar respostas a incidentes de segurança, com o objetivo de proteger ativos de informação e garantir a confidencialidade, integridade e confidencialidade dos dados do TJCE (*Blue Team*). Os detalhes técnicos e operacionais são apresentados no **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

b) Serviço de gestão testes de invasão (*Red Team*): Serviço de execução de avaliações de segurança e testes de invasão, internos e externos, nos sistemas, aplicativos e infraestrutura do TJCE, com o objetivo de identificar vulnerabilidades, avaliar a eficácia das medidas de segurança implementadas e solicitar implementações das vulnerabilidades encontradas (*Red Team*). Os detalhes técnicos e operacionais são apresentados no **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

c) Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação: Serviços gerenciados de monitoramento e correlação de eventos, por meio de correlacionamento de *logs*, pacotes de redes e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, para detectar, analisar e responder a ameaças de segurança por meio do monitoramento e análise centralizado de logs de todos os ativos de rede atuais e considerados em demandas futuras do TJCE, usando a ferramenta SIEM com quantidade mínima de funcionamento de 3.000 EPS. Os detalhes técnicos e operacionais são apresentados no **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

§2° ESPECIFICAÇÃO TÉCNICA

I. Conforme consta no **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

§3° MODELO DE EXECUÇÃO DO OBJETO

I. Após a assinatura do contrato, será agendada uma reunião de alinhamento como primeira etapa do período de transição. O objetivo dessa reunião é facilitar a transferência de conhecimentos e a transição dos serviços para a CONTRATADA.

II. A CONTRATADA deverá implantar os serviços, no prazo máximo de 30 dias corridos após assinatura de contrato e Ordem de Serviço das soluções contratadas com, pelo menos, os seguintes requisitos atendidos e documentados em um relatório de implantação:

a) Lotação de todos os profissionais alocados por perfil (com a devida documentação comprobatória conforme itens 2.4, 3.4 e 4.8 do **ANEXO I – Serviços Gerenciados de Segurança da Informação**) para os horários de expediente regular e de plantão contínuo.

b) Comprovação da disponibilidade de uso dos recursos de TI descritos no item 1.3.6 do **ANEXO I – Serviços Gerenciados de Segurança da Informação** para viabilização de imediata prestação de serviços.

c) Relatório técnico produzido através da ferramenta SIEM, comprovando**:**

i. Coleta de logs efetuada pelo Coletor *on-premise*, conforme descrito nos itens (com subitens) de 4.2 e 4.3 do **ANEXO I – Serviços Gerenciados de Segurança da Informação**.

ii. Regras preestabelecidas, normalização e correlação de eventos conforme o item (com subitens) de 4.4. do **ANEXO I – Serviços Gerenciados de Segurança da Informação**.

iii. Capacidade de emitir alertas e notificações conforme item (com subitens) 4.2 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

iv. Ter inicializado o armazenamento de logs conforme item 4.2.19 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

v. Apresentar o *Dashboard* em funcionamento conforme os itens (com subitens) 4.2.30, 4.2.31 e 4.2.32 do **ANEXO I – Serviços Gerenciados de Segurança da Informação**.

vi. Console de administração e operação do SIEM em funcionamento conforme item (com subitens) 4.5.3 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

III. Após a implantação, o TJCE emitirá um Termo de Recebimento Provisório (TRP) e em até 5 dias úteis validará a implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Caso a validação indique pendências de implantação, a CONTRATADA deverá executar as retificações em até 15 dias corridos.

IV. Após a validação sem pendências da implantação, será assinado o Termo de Recebimento Definitivo (TRD) de implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Somente a partir da assinatura do TRD, a execução dos serviços será considerada inicializada para finalidade de pagamento, o qual será mensal e sujeito a glosas conforme Tabela 5 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

V. Até 30 dias corridos após o TRD de implantação, a CONTRATADA deve apresentar um plano de trabalho anual com atividades mensais a serem executadas pelos membros do *Blue*/*Red Team* e a equipe de Serviços gerenciados de monitoramento e correlação de eventos. O plano de trabalho deverá ser validado pela equipe de segurança do TJCE e poderá ser modificado sob demanda da equipe de segurança do TJCE em qualquer momento.

VI. O período inicial de 90 (noventa) dias corridos, após a assinatura do TRD de implantação, será considerado como período de estabilização da operação dos serviços, durante o qual os indicadores de serviço não atingidos terão aplicadas as glosas de Tabela 4 e Tabela 5 do **ANEXO I – Serviços Gerenciados de Segurança da Informação** para todos os serviços contratados, conforme os seguintes critérios em dias corridos:

a) Nos primeiros 30 (trinta) dias: não serão aplicadas as glosas previstas nas Tabelas 4 e 5 do **ANEXO I** para cada ocorrência de indicador de serviço não atingido.

b) Do 31º ao 60º dia: aplicar-se-á efetivamente 25% (cinquenta por cento) dos pontos previstos em Tabela 4 e Tabela 5 do **ANEXO I** para cada ocorrência de indicador de serviço não atingido. Nesta etapa todos os serviços descritos nos itens 2, 3 e 4 do **ANEXO I** devem estar totalmente configurados corretamente.

c) Do 61º ao 90º dia: aplicar-se-á efetivamente 50% (setenta e cinco por cento) dos pontos previstos em Tabela 4 e Tabela 5 do **ANEXO I** para cada ocorrência de indicador de serviço não atingido.

d) Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos em Tabela 4 e Tabela 5 do **ANEXO I** para cada ocorrência de indicador de serviço não atingido.

e) Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização.

VII. Reunião de Alinhamento e entrega do cronograma

a) O coordenador do SOC, em conjunto com o *Blue*/*Red Team* e a equipe de Serviços gerenciados de monitoramento e correlação de eventos (ver Tabela 2 do **ANEXO I – Serviços Gerenciados de Segurança da Informação**), deve apresentar mensalmente um relatório contendo as atividades executadas pelo SOC, as quais devem ser correlacionadas com as atividades do plano de trabalho anual constante neste documento. Para o primeiro mês, o relatório deverá conter um diagnóstico do estado de maturidade da segurança da informação do TJCE e as ações a serem executadas no plano de trabalho proposto.

b) Um resumo das atividades rotineiras por equipe, unidade de prestação de serviços e frequência de serviços é mostrada na seguinte Tabela**.** Vale a pena ressaltar que a descrição detalhada dos serviços contratados está nos itens 2, 3 e 4 do **ANEXO I.**

Serviço	Atividade Operacional	Unidade	Frequência
1	**Serviço de gestão de incidentes de segurança (*Blue Team*):** Análise, resolução, controle e documentação de eventos e incidentes de segurança da informação, seguindo os principais Frameworks de gestão de incidentes de segurança da informação e as melhores práticas de mercado.	Mensal	Rotineiro ou por Requisição de Serviço
2	**Serviço de gestão testes de invasão (*Red Team*):** Identificar, mapear e documentar potenciais vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Para realizar esses testes, são utilizadas técnicas e ferramentas específicas com o intuito de simular a obtenção de acesso não autorizado e privilegiado aos ativos e informações. Além disso, o serviço também fornece recomendações para corrigir as vulnerabilidades identificadas, visando fortalecer a segurança dos sistemas e proteger os ativos e dados sensíveis.	Mensal	Requisições de Serviço
3	**Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação:** Realizar o monitoramento constante e ininterrupto dos ativos de segurança da informação, assim como de ataques cibernéticos direcionados ao TJCE. Serviço a ser realizado por meio do correlacionamento de logs, pacotes de rede e detecção de comportamentos anômalos em aplicações, serviços e infraestrutura com a ferramenta tecnológica SIEM. As atividades têm como objetivo identificar eventos de segurança da informação, que serão analisados e podem ser classificados como incidentes de segurança, conforme estabelecido no processo de gestão de incidentes.	Mensal	Rotineiro ou por Requisições de Serviço

c) Após a emissão do TRD de implantação, o coordenador do SOC, em conjunto com o *Blue*/*Red Team* e a equipe de serviços gerenciados de monitoramento e correlação de eventos

(ver Tabela 2 do **ANEXO I**), devem apresentar semanal e mensalmente, em reunião, um resumo do estado geral de segurança do TJCE, contendo: eventos, incidentes e vulnerabilidades relevantes da rede, trabalhos futuros de mitigação e estado do andamento das atividades rotineiras e sob demanda, as quais devem ser vinculadas com o plano de trabalho do SOC.

d) As requisições de serviço poderão ser abertas a qualquer momento, independentemente do horário ou do dia, incluindo dias úteis, finais de semana, feriados e pontos facultativos, e deverão ser executados em conformidade com os níveis de serviços estabelecidos no **ANEXO I.**

e) A CONTRATADA deverá disponibilizar todas as informações essenciais para a transição para uma possível e futura NOVA CONTRATADA, no prazo mínimo de 30 dias corridos antes do fim do contrato, desde que não seja efetivada a renovação do contrato. Além disso, será responsável por elaborar e atualizar toda a documentação necessária que possa não ter sido adequadamente gerada ou atualizada durante a vigência do contrato.

VIII. Local de execução do serviço

a) A execução dos serviços, assim como entrega e instalação dos equipamentos deverá ocorrer no seguinte endereço, após agendamento prévio com o fiscal técnico ou seu substituto: Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza – CE, 60811-690.

IX. Forma de avaliação da qualidade dos bens e/ou serviços entregues

a) Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, o TJCE, através do Fiscal Técnico, realizará, anualmente, a Avaliação de Desempenho, o que permitirá a adoção de eventuais ajustes no modelo de atendimento, conforme critérios abaixo, podendo ser criados outros que se fizerem necessários.

b) **Comunicação:** Avaliação qualitativa da comunicação do Contratado, como clareza na informação, formas de solicitações e questionamentos ao TJCE, educação e nível de formalidade no atendimento e tempo de resposta às solicitações.

c) **Confiabilidade:** Prestação correta (isenta de falhas e erros) do serviço/atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas.

d) **Organização:** Demonstração de planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

e) Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos seguintes conceitos: Péssimo (de 0 a 4,9) / Regular (de 5 a 7,4) / Bom (de 7,5 a 8,9) / Ótimo (de 9 a 10).

f) Anualmente, a empresa contratada será informada do conceito médio obtido no período e registrado nos autos do contrato, resultado este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

X. Todas as informações relevantes para o dimensionamento da proposta estão detalhadas no item 4.6 **ANEXO I**.

XI. O horário e regime de execução do serviço é detalhado no item (com subitens) 1.3 do **ANEXO I.**

XII. Medição de resultados

a) Os serviços serão medidos, controlados e acompanhados pela Contratante durante o período de vigência do contrato de acordo com os Níveis Mínimos de Serviço (NMS) e suas respectivas notificações ou penalidades, as quais estão detalhadas no item 5 do **ANEXO I**.

XIII. Mecanismos formais de comunicação

a) A metodologia adotada para a requisição de serviços está detalhada no item 1.6 do **ANEXO I**.

b) A CONTRATADA deverá emitir mensalmente, junto ao pedido de pagamento, o Relatório de Níveis Mínimos de Serviços, constando indicadores de requisições de serviços,

NMS e chamados técnicos abertos, em andamento e encerrados no período, com no mínimo as seguintes informações:

i. Número do contrato.
ii. Fiscal técnico responsável.
iii. Número de chamado.
iv. Descrição da ocorrência.
v. Severidade.
vi. Nome de quem registrou o chamado ou solicitou abertura do chamado.
vii. Data e hora de abertura do chamado.
viii. Data e hora do início do atendimento.
ix. Data e hora do atendimento local, se for o caso.
x. Data e hora de solução ou medida de contorno.
xi. Descrição da resolução adotada.

c) Os relatórios deverão ser entregues mesmo quando não houver chamados/ocorrências no período.

d) Após a análise e aprovação do relatório descrito no item anterior, a Contratante deverá emitir o documento "Autorização para Faturamento", descrito no próximo item deste Termo de Contrato.

e) Autorização para Faturamento: Autorização emitida pelo Fiscal Administrativo do Contrato ao Preposto da Contratada. Este documento contém a autorização para que a Contratada possa efetuar o faturamento.

XIV. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

a) A garantia contratual dos serviços, complementar à garantia legal, deve atender as especificações técnicas do item 4 e os NMS descritos no item 5 do **ANEXO I**, pelo prazo mínimo contratual de 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do TRD.

CLÁUSULA QUINTA – DO PREÇO, PRAZO E CONDIÇÕES DE PAGAMENTO

A CONTRATANTE pagará à CONTRATADA, pelos serviços prestados, o valor global anual de **R$ 4.939.999,84 (quatro milhões, novecentos e trinta e nove mil, novecentos e noventa e nove reais e oitenta e quatro centavos)**, referente aos serviços descritos no Anexo I deste Termo de Contrato.

§ 1º A CONTRATADA deverá observar, quanto aos prazos, custo e forma de pagamento, as seguintes diretrizes:

I. Os pagamentos serão realizados através de depósito bancário, preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento mensal e definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade com as medições realizadas, validado previamente pela CONTRATANTE atestada pelo setor competente deste Tribunal de Justiça, via emissão do Termo de Recebimento Definitivo, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

II. O prazo para pagamento de faturas ou notas fiscais serão suspensos durante o período de indisponibilidade do sistema de pagamento do Estado do Ceará ao final de cada exercício financeiro, aproximadamente entre 20 de dezembro e 31 de janeiro do ano subsequente, cujos pagamentos serão realizados até o final da primeira quinzena do mês de fevereiro.

III. O Tribunal de Justiça reserva-se ao direito de recusar o pagamento, no ato do atesto, caso o objeto não esteja em conformidade com as condições deste instrumento.

IV. Nenhum pagamento será efetuado à empresa antes regularizada as sanções que por ventura lhe tenham sido aplicadas.

V. Nas notas fiscais referentes aos serviços objeto do contrato, deverão estar descriminados os valores dos tributos: impostos sobre serviços – ISS, PIS/PASEP, COFINS, FUST, FUNTTEL.

VI. Os serviços de suporte e manutenção serão faturados mensalmente após a solicitação de pagamento por parte da CONTRATADA, sendo o pagamento condicionado ao aceite do Relatório de Instrumento de Medição de Resultados, conforme **alínea b, inciso XIII, parágrafo 3° da Cláusula Quarta** por parte da CONTRATANTE:

a) O valor do pagamento mensal estará diretamente vinculado ao índice alcançado para os indicadores estabelecidos, sendo pago conforme resultado obtido e decrementado (cumulativamente) quando não forem atingidas as metas exigidas.

b) Caso a CONTRATADA não cumpra com os seus compromissos, de qualidade e desempenho, terá a sua fatura reduzida conforme estabelecido nas Glosas apresentadas no item 5 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

c) Os redutores deverão ser levantados pela Contratada, anexados à solicitação de pagamento, sendo validados pelo TJCE. Os redutores serão aplicados sobre o faturamento mensal na ocorrência dos fatos geradores, independentemente da abertura de processo administrativo.

VII. Constatada a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

VIII. Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

IX. Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

X. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação

XI. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

XII. Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) estar em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

XIII. O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual.

XIV. Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

XV. Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

XVI. A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

§ 2º Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}00016438$$

no qual i = taxa percentual anual no valor de 6% (seis por cento).

CLÁUSULA SEXTA – DO REAJUSTE E DOS RECURSOS ORÇAMENTÁRIOS

A CONTRATANTE atenderá às prescrições para reajustamento do contrato nos termos definidos nesta cláusula.

§ 1º Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de apresentação da proposta.
§ 2º Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do **Índice de Custo da Tecnologia da Informação (ICTI) - Ipea**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
§ 3º O processo referente ao pedido de reajuste supra, deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.
§ 4º Os recursos financeiros serão decorrentes do financiamento contraído junto ao Banco Interamericano de Desenvolvimento – BID, no âmbito do Programa de Modernização do Poder Judiciário do Estado do Ceará (PROMOJUD), tendo como fonte os Recursos de Operações de Crédito, nas seguintes dotações orçamentárias:

04100021.02.126.512.15504.15.339040.1.754.3220059.1.20 (06940)

CLÁUSULA SÉTIMA – DOS ELEMENTOS PARA GESTÃO DO CONTRATO

Os elementos para a gestão do contrato serão processados da seguinte forma:

§ 1º Forma de Acompanhamento do Contrato:

ID	Evento	Forma de Acompanhamento
1	Da entrega da solução	O recebimento do objeto deverá ocorrer conforme definido no **parágrafo 3° da Cláusula Quarta** deste Termo de Contrato.
2	Durante a vigência do Contrato	Será verificado o cumprimento do prazo de solução dos chamados, conforme descrito no item 5 do **ANEXO I – Serviços Gerenciados de Segurança da Informação.**

§ 2º Prazos e Condições

I. Os prazos são detalhados na seguinte Tabela:

N.	Etapa	Quando	Responsável
1	Assinatura do contrato	Após a homologação do certame.	CONTRATANTE e CONTRATADA
2	Implantação dos serviços conforme os requisitos apresentados no **inciso II, parágrafo 3° da Cláusula Quarta** deste Termo de Contrato por parte da CONTRATADA e entrega do TRP da CONTRATANTE para a CONTRATADA.	Em até 30 (trinta) dias corridos contados após a assinatura do contrato.	CONTRATANTE e CONTRATADA
3	Validação da implantação dos serviços (etapa anterior) mediante a emissão do TRD da CONTRATANTE para a CONTRATADA em caso de não possuir pendências ou solicitação de retificações para que a CONTRATADA efetue as correções e solicite um novo TRP (volta a Etapa 2).	Em até 5(cinco) dias úteis após a emissão do TRP.	CONTRATANTE
4	Início do período de validade/vigência dos serviços.	A partir da data de emissão do TRD.	CONTRATADA

II. Condições conforme o **parágrafo 3° da Cláusula Quarta** deste Termo de Contrato.

§ 3º Estimativa do Volume de Bens/Serviço:

ID	Demanda Prevista	Quantitativo a ser contratado
1	Serviço de gestão de incidentes de segurança (*Blue Team*)	1 Unidade/Serviço
2	Serviço de gestão testes de invasão (*Red Team*)	1 Unidade/Serviço
3	Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação	1 Unidade/Serviço
4	Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.	10 Unidades/Serviço
5	Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.	10 Unidades/Serviço

6	Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.	10 Unidades/Serviço

I. As demandas previstas com IDs 4, 5 e 6 da Tabela mostrada acima poderão ser contratadas opcionalmente, sob demanda de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual.

II. Não haverá obrigação do TJCE, na utilização do quantitativo parcial ou total dos pacotes de extra que são apresentadas nas demandas previstas com IDs 4, 5 e 6 apresentadas na Tabela anterior.

§ 4º Propriedade, sigilo e restrições:

I. A CONTRATADA cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do Art. 93, da LEI Nº 14.133, DE 1º DE ABRIL DE 2021, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência do objeto contratado, entendendo-se por resultados quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros.

II. Toda a documentação produzida pela CONTRATADA referente à implantação dos equipamentos e documentos exigidos no termo de referência passam a ser propriedade de forma perpétua do TJCE, não precisando este Tribunal de autorização da CONTRATADA para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

III. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados (em outros contratos) pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso.

IV. A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente.

V. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados que, a qualquer título, venham a integrar a equipe executante do Objeto, a assinatura do **ANEXO II – TERMO DE CIÊNCIA**, bem como a assinatura do **ANEXO III – TERMO DE COMPROMISSO**, onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

VI. A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte, mediante assinatura do Termo de Confidencialidade constante no Termo de Contrato.

§ 5º Mecanismos formais de comunicação:

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade

Emissão da Requisição de serviço/fornecimento	Contratante	Contratada	Requisição de serviço/fornecimento	Quando demandado pela SETIN.
Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, *email*, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*PortableDocument Format*): documento em formato portável.	Quando necessário

CLÁUSULA OITAVA – DA GARANTIA DOS SERVIÇOS

A especificação da garantia do serviço deverá observar o art. 40, §1º, inciso III, da Lei nº 14.133, de 2021.

§ 1º A garantia contratual dos serviços, complementar à garantia legal, deve atender as especificações técnicas do item 4 e os Níveis Mínimos de Serviço (NMS) descritos no item 5 do **ANEXO I – Serviços Gerenciados de Segurança da Informação**, pelo prazo mínimo contratual de 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do Termo de Recebimento Definitivo (TRD).

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

A Adjudicatária deverá oferecer, a título de garantia do contrato, a partir da data de homologação, e conforme o Art. 98, da Lei nº 14.133/2021 e suas alterações, 5% (cinco por cento) do valor anual do contrato, devidamente atualizado.

§ 1º Será concedido prazo mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para a prestação da garantia pelo contratado quando optar pela modalidade seguro-garantia. As demais modalidades deverão ser apresentadas em até 5 (cinco) dias, a contar da assinatura do Termo de Homologação.

§ 2º A garantia prestada será restituída e/ou liberada **90 (noventa) dias** após o término da vigência contratual, desde que cumpridas integralmente todas as obrigações contratuais; quando em dinheiro, será atualizada monetariamente, conforme dispõe o art. 100, da Lei nº. 14.133/2021.

§ 3º Poderá o contratado optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, nos termos do art. 96, § 1º, da Lei 14.133/2021.

§ 4º A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual.

§ 5º Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

§ 6º A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

I. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

II. Prejuízos diretos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

III. Multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

IV. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

§ 7º No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

§ 8º Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

I. A não complementação ou renovação, tempestiva, da garantia do contrato ensejará a suspensão de pagamentos até a regularização do respectivo documento, independentemente da aplicação das sanções contratuais.

II. A inobservância do prazo fixado para apresentação, complementação ou renovação da garantia acarretará a aplicação das sanções previstas neste Termo de Contrato.

§ 9º O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

§10 O emitente da garantia ofertada pela contratada deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

§11 Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

§12 Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato;

§13 A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

§14 A garantia somente será liberada ante a comprovação de que o contratado pagou todas as verbas rescisórias decorrentes da contratação, sendo que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia deverá ser utilizada para o pagamento dessas verbas trabalhistas, incluindo suas repercussões previdenciárias e relativas ao FGTS, observada a legislação que rege a matéria;

§15 Também poderá haver liberação da garantia se a empresa comprovar que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de

trabalho;

§16 Por ocasião do encerramento da prestação dos serviços contratados, a Administração Contratante poderá utilizar o valor da garantia prestada para o pagamento direto aos trabalhadores vinculados ao contrato no caso da não comprovação: (1) do pagamento das respectivas verbas rescisórias ou (2) da realocação dos trabalhadores em outra atividade de prestação de serviços.

§17 O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

§18 A CONTRATADA autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no Contrato.

CLÁUSULA DEZ – DAS SANÇÕES ADMINISTRATIVAS

Quanto às sanções administrativas, deve-se observar o disposto nesta cláusula.

§1° Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a contratado que:

I. der causa à inexecução parcial do contrato;

II. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

III. der causa à inexecução total do contrato;

IV. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

V. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

VI. praticar ato fraudulento na execução do contrato;

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

VIII. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

§2° Serão aplicadas à contratada que incorrer nas infrações acima descritas as seguintes sanções:

I. Advertência, quando a contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art.156, §2º, da Lei nº 14.133, de 2021);

II. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos **incisos II, III e IV do §1º desta Cláusula**, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos **incisos V, VI, VII e VIII do §1º desta Cláusula**, bem como nos **incisos II, III e IV**, que justifiquem a imposição de penalidade mais grave (art.156, §5º, da Lei nº 14.133, de 2021);

IV. Multa:

a) **moratória:**

i. Caso a CONTRATADA se torne inadimplente na execução dos serviços, o CONTRATANTE poderá, sem prejuízo de outras medidas, a título de multa, o equivalente a 0,5% (cinco décimos por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, para a conclusão da demanda, nos termos e condições dispostas neste Termo de Contrato, sem prejuízo das sanções legais e responsabilidades civil e criminal.

ii. Na ordem de 0,5% do valor total da contratação, ao dia de suspensão ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços contratados ao total de 10%, moratório.

iii. Caso os limites do subitem anterior sejam excedidos, configura-se então casos de inexecução contratual.

b) **compensatória** (aplicação de multa administrativa, além das glosas previstas neste documento e seus anexos):

i. Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo.

§3° A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

§4° A aplicação das sanções previstas no contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE (art. 156, §9º, da Lei nº 14.133, de 2021).

§5° Todas as sanções previstas poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021):

I. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art.157, da Lei nº 14.133, de 2021);

II. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo CONTRATANTE à CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art.156, §8º, da Lei nº 14.133, de 2021);

§6° A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto no caput e parágrafos do art.158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar**.**

§7° Na aplicação das sanções serão considerados (art.156, §1º, da Lei nº 14.133, de 2021)**:**

I. a natureza e a gravidade da infração cometida;

II. as peculiaridades do caso concreto;

III. as circunstâncias agravantes ou atenuantes;

IV. os danos que dela provierem para a Administração Pública;

V. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

§8° A personalidade jurídica da CONTRATADA poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art.160, da Lei nº 14.133, de 2021).

§9° O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal. (art.161, da Lei nº 14.133, de 2021).

§10 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art.163 da Lei nº 14.133/21

§11 Os débitos da CONTRATADA para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes do contrato ou de outros contratos administrativos que a CONTRATADA possua com o mesmo órgão contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

§12 Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis,

encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.
§13 Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.
§14 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
§15 A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.
§16 Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.
§17 As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.
§18 A sanção de multa calculada na forma deste Termo de Contrato, não será inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.
§19 A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.
§20 Os percentuais de multas aplicadas incidirão sobre o valor global do termo de contrato licitado ou celebrado, quando moratórias.
§21 Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

CLÁUSULA ONZE – DA EXTINÇÃO CONTRATUAL

O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.
§ 1º Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.
§ 2º Quando a não conclusão do contrato referida no parágrafo anterior decorrer de culpa da CONTRATADA:

I. Ficará ela constituída em mora, sendo-lhe aplicáveis as respectivas sanções administrativas;
II. Poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

§ 3º O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

I. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.
II. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.
III. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

§ 4º A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput,* da Lei n.º 14.133, de 2021).
§ 5º O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do

contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DOZE – DA SUBCONTRATAÇÃO

Não será permitida a subcontratação total ou parcial do objeto deste Termo de Contrato.

§1° Não será admissível a fusão, cisão ou incorporação da CONTRATADA.

CLÁUSULA TREZE – DOS CRITÉRIOS AMBIENTAIS

A CONTRATADA deverá providenciar o recolhimento e o adequado descarte de produto(s) e material(is) inservível(is) originário(s) da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA n° 01, de 18/03/2010, da Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA n° 416, de 30/09/2009, e legislação correlata.

§1º A CONTRATADA deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 11º da Lei n.º 14.133/21.
§2º Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.
§3º Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.
§4º Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva ROHS (*restriction of certain hazardous substances*), tais como mercúrio (hg), chumbo (pb), cromo hexavalente (cr(vi)), cádmio (cd), bifenil-polibromados (pbbs), éteres difenil-polibromados (pbdes).
§5º Os serviços prestados e os bens fornecidos pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

CLÁUSULA QUATORZE – DO PRAZO DE VIGÊNCIA DO CONTRATO

O prazo de vigência deste termo de contrato será de 36 (trinta e seis) meses, contados da assinatura do CONTRATO, podendo ser prorrogado até limite permitido pela Lei 14.133/21, e conforme a conveniência estabelecida entre CONTRATADA e CONTRATANTE.

CLÁUSULA QUINZE – DO GESTOR DO CONTRATO E DO ORDENADOR DE DESPESAS

O órgão responsável pela contratação é o Tribunal de Justiça do Estado do Ceará.

§ 1º O Gestor do Contrato será a(o) Secretária(o) de Tecnologia da Informação do TJCE ou profissional por ela(e) indicado devidamente oficializado por meio de publicação no Diário da Justiça Eletrônico.
§ 2º Os Ordenadores de Despesas serão o(a) Desembargador(a) Presidente do Tribunal de Justiça do Estado do Ceará conjuntamente com a(o) Secretária(o) de Tecnologia da Informação do TJCE, conforme Portaria n. 310/2023, disponibilizada no DJe de 09 de fevereiro de 2023, que dispõe sobre a delegação de competências administrativas no âmbito do Poder Judiciário do Estado do Ceará.

CLÁUSULA DEZESSEIS – DAS ALTERAÇÕES CONTRATUAIS

As alterações ao presente contrato poderão ser necessárias se ocorrerem quaisquer das situações previstas no artigo 124 da Lei Federal nº 14.133/21.

PARÁGRAFO ÚNICO – A CONTRATADA deverá aceitar, nas mesmas condições propostas, os acréscimos ou as supressões que se fizerem necessária, até o limite de 25% do valor inicial do contrato, nos termos do artigo 125 da Lei n° 14.133/21.

CLÁUSULA DEZESSETE – DA LEGISLAÇÃO APLICÁVEL

Este termo de contrato rege-se pela Lei n° 14.133/21 e suas alterações, pela legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

CLÁUSULA DEZOITO – DA PROTEÇÃO DE DADOS PESSOAIS

§ 1º As Partes se comprometem a cumprir todas as leis, regras e regulamentos aplicáveis aos dados pessoais tratados em razão da execução das obrigações assumidas por elas neste instrumento, incluindo, mas não se limitando, a Lei 13.709/18 (Lei de Proteção de Dados Pessoais – LGPD).

§ 2º As Partes se obrigam a utilizar os dados pessoais eventualmente recebidos em função desta relação jurídica somente para a finalidade ajustada neste instrumento, não podendo, em nenhum caso, utilizar esses dados pessoais para finalidade distinta, sob pena de rescisão imediata e assunção integral de quaisquer danos causados à outra Parte e/ou a terceiros.

§ 3º As Partes desde já concordam e autorizam expressamente que a outra realize a transferência dos dados pessoais recebidos em razão da relação jurídica, somente para empresas cujas atividades sejam relacionadas, direta ou indiretamente, às finalidades deste contrato: prestadoras de serviços contábeis, instituições bancárias, órgãos da administração pública, dentre outros.

§ 4º Extintas as obrigações do presente contrato, as Partes se obrigam a não armazenar e a não compartilhar os dados pessoais objeto do contrato com terceiros, salvo com autorização prévia e expressa da outra Parte ou para o cumprimento de legítimo interesse, obrigação legal ou regulatória pelo Controlador, pelo prazo legalmente previsto em lei.

§ 5º As Partes estão cientes do seu dever e obrigação legal de orientar seus funcionários, terceiros e parceiros a agirem conforme a Lei Geral de Proteção de Dados Pessoais.

CLÁUSULA DEZENOVE – DA PUBLICAÇÃO

Incumbirá ao CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário da Justiça eletrônico (DJe), no prazo previsto na Lei n. 14.133/2021.

CLÁUSULA VINTE – DA POSSIBILIDADE DO PETICIONAMENTO PELO PORTAL DO TJCE

Em caso de eventuais demandas da contratada, o novo Portal de Atendimento do TJCE para protocolo exclusivamente administrativo (CPA) permitirá consultas processuais, petições iniciais e intermediárias no âmbito dos processos administrativos, desde que realize cadastro prévio no Portal (https://portaladmin.tjce.jus.br/atendimento/) e possua certificado digital.

Visando a facilitar a utilização do Portal, foram disponibilizados 3 (três) vídeos tutoriais, cujos links seguem abaixo:

1) Cadastro de Usuário:
https://www.youtube.com/watch?v=J00Yow2ywRc

2) Peticionamento Inicial:
https://www.youtube.com/watch?v=TNhHA6vQKdg

3) Peticionamento Intermediário:
https://www.youtube.com/watch?v=dT5pLHNwXyw

Os vídeos tutoriais referenciados constarão do site do TJCE (https://www.tjce.jus.br/) de forma permanente.

CLÁUSULA VINTE E UM – DO FORO

Fica eleito o foro de Fortaleza (CE), para dirimir quaisquer dúvidas oriundas do presente Termo de Contrato, caso não possam ser resolvidos por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

PARÁGRAFO ÚNICO – Firmam o presente em 2 (duas) vias de igual teor e forma, por estarem justos e acertados, na presença da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça Eletrônico (DJe).

Fortaleza, data da última assinatura registrada pelo sistema.

ANTONIO ABELARDO BENEVIDES MORAES:11613297300
Assinado de forma digital por ANTONIO ABELARDO BENEVIDES MORAES:11613297300
Dados: 2024.03.27 18:51:47 -03'00'

Desembargador Antônio Abelardo Benevides Moraes
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ

DENISE MARIA NOROES OLSEN:28381610320
Assinado de forma digital por DENISE MARIA NOROES OLSEN:28381610320
Dados: 2024.03.22 14:52:58 -03'00'

Denise Maria Norões Olsen
SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO DO TJCE

ASSINADO DIGITALMENTE
YURE LEOPOLDO SABINO DE FREITAS
A conformidade com a assinatura pode ser verificada em: http://serpro.gov.br/assinador-digital
SERPRO

Yure Leopoldo Sabino De Freitas
REPRESENTANTE DA EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

Testemunhas:

1._____
RG:
CPF:

2._____
RG:
CPF:

ANEXO I DO CONTRATO

SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO

TRF ANEXO I

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

Os serviços gerenciados de segurança da informação serão compostos pelos serviços mostrados na seguinte Tabela.

Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação

LOTE	SERVIÇO	DESCRIÇÃO DO SERVIÇO	QTD
1	1	**Serviço de gestão de incidentes de segurança (Blue Team), por 36 meses.**	1
	2	**Serviço de gestão testes de invasão (Red Team), por 36 meses.**	1
	3	**Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS por 36 meses.**	1
	4	**Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.**	10
	5	**Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.**	10
	6	**Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.**	10

1. REQUISITOS OPERACIONAIS MÍNIMOS DO SOC

1.1. O Security Operations Center (SOC) é uma unidade essencial para a segurança da informação, composta por diferentes equipes especializadas. O Blue Team é responsável pela defesa e monitoramento contínuo dos sistemas e redes, detectando e respondendo a incidentes de segurança. O Red Team realiza testes de penetração e simula ataques para identificar vulnerabilidades e pontos fracos, fortalecendo as defesas. O serviço de monitoramento e correlação de eventos, com o uso de uma ferramenta SIEM, coleta e analisa dados de segurança em tempo real, detectando padrões suspeitos e atividades maliciosas. Essa combinação de Blue Team, Red Team e serviço de monitoramento e correlação de eventos permite uma abordagem abrangente de segurança, fortalecendo a postura de defesa, antecipando e respondendo a ameaças, e garantindo a proteção dos ativos de um órgão ou organização.

1.2. O Blue Team comandará as operações no SOC. O SOC deve ser composto por profissionais de segurança da informação altamente qualificados para desempenhar várias funções cruciais e garantir a proteção e integridade dos recursos computacionais do TJCE.

1.3. A prestação de todos os serviços descritos neste Anexo deve ser realizada conforme:

1.3.1. Horário de expediente regular: Durante os dias úteis e de segunda a sexta-feira, com carga horária diária de 8h, entre 7h e 19h de acordo a definição do TJCE e de forma remota, com exceção da presencialidade do Red Team para atividades de testes de intrusão envolvendo acesso físico à rede ou segurança física (sob demanda do TJCE e com antecedência mínima de 30 dias corridos). Neste horário, a CONTRATADA deverá prestar serviços com no mínimo 1 (um) profissional por perfil (ver Tabela 2. Força de Trabalho Orientativa). Não haverá expediente forense nos feriados nacionais, estaduais e municipais, bem como nas datas determinadas pela Presidência do Tribunal de Justiça, formalizadas através de portaria publicada no Diário da Justiça Eletrônico. O recesso natalino compreendido entre os dias 20 de dezembro e 06 de janeiro deverá ser considerado como dia útil para prestação dos serviços, mesmo não ocorrendo o expediente forense.

1.3.2. Horário de plantão contínuo: Deverá estar disponível em regime de plantão contínuo e fora do horário de expediente regular, 24 horas por dia, 7 dias por semana e durante todos os 365 dias do ano de forma remota, no mínimo 1 (um) profissional da equipe do Blue Team e 1 (um) profissional da equipe Serviço de monitoramento e correlação de eventos (ver Tabela 2. Força de Trabalho Orientativa) para lidar com solicitações de serviços relacionados a incidentes ou desastres de sistemas críticos e tratamento de incidentes no ambiente computacional do TJCE.

1.3.3. Todos os profissionais devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

1.3.4. Será adotado um método de trabalho fundamentado no princípio de delegação de responsabilidade para a execução dos serviços. Esse princípio estabelece que o TJCE será responsável pela gestão do contrato e pela verificação do cumprimento dos padrões de qualidade exigidos para os serviços entregues, enquanto a CONTRATADA será responsável pela execução dos serviços e pela gestão dos profissionais sob sua responsabilidade.

1.3.5. A CONTRATADA terá a responsabilidade de executar os serviços e realizar um acompanhamento diário para garantir a qualidade e o cumprimento dos níveis de

serviço estabelecidos. Caso surjam problemas que possam prejudicar a eficiência dos serviços ou a alcançar os níveis de serviço acordados, essas questões devem ser prontamente comunicadas por escrito ao TJCE, a fim de tomar as medidas necessárias para ajustes e correções.

1.3.6. A CONTRATADA deve ser responsável por fornecer ao(s) integrante(s) do Blue/Red Team e do Serviço de monitoramento e correlação de eventos, as devidas ferramentas computacionais de trabalho no ambiente remoto ou presencial pré-agendado (Red Team): computador/laptop, servidores, telas de monitoramento, periféricos computacionais, hardware e software licenciado, assim como demais ativos computacionais necessários.

1.3.7. Para garantir a segregação adequada de funções e promover a efetividade das equipes envolvidas, fica estabelecido que os integrantes de cada equipe, ou seja, do Blue Team, Red Team e Serviços de monitoramento e correlação de eventos, não poderão exercer atividades simultaneamente em mais de um perfil (ver Tabela 2. Força de Trabalho Orientativa). Cada profissional deve ser alocado exclusivamente em um perfil, com responsabilidades específicas e atribuições relacionadas à sua respectiva função. É de responsabilidade da contratada garantir o cumprimento desta exigência, assegurando que nenhum integrante atue em mais de um perfil ou equipe. Este requisito tem como objetivo principal fortalecer a especialização de cada perfil por equipe, garantindo o adequado desempenho das atividades e a maximização dos resultados alcançados no âmbito do SOC.

1.3.8. Com o objetivo de aprimorar a precisão das informações de suporte para a elaboração das propostas, foi disponibilizado um quadro que apresenta a Força de Trabalho Orientativa para os perfis profissionais que serão alocados no TJCE, com suas respectivas quantidades. Vale ressaltar que o dimensionamento da força de trabalho por perfil é de total responsabilidade da empresa contratada:

Tabela 2. Força de Trabalho Orientativa

Perfil	Quantidade Mínima de Profissionais por Equipe	Equipe
Especialista em Segurança	1	Blue Team
Analista de Segurança Pleno	1	Blue Team
Analista de Segurança Sênior	1	Red Team
Analista de Segurança Pleno	1	Serviço de monitoramento e correlação de eventos

1.3.9. Considerando que a prestação do serviço é baseada em níveis mínimos de serviço, a Tabela 2. Força de Trabalho Orientativa é informativa. O quantitativo apresentado foi

baseado na força de trabalho prevista que tem como escopo os serviços de gestão dos ativos de rede que fazem parte do parque tecnológico de segurança da informação do TJCE, conforme mostrado na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE.

1.4. A CONTRATADA é responsável por manter as licenças de software proprietário, que serão usados nos serviços mostrados nos itens 2, 3 e 4, ativas e válidas, devendo apresentar ao TJCE uma cópia autenticada dessas licenças anualmente.

1.5. A CONTRATADA é responsável pelo correto funcionamento dos equipamentos usados por ela para a prestação dos serviços mostrados nos itens 2, 3 e 4, sem custos adicionais para o TJCE.

1.6. A CONTRATADA deverá realizar todas suas atividades com o suporte de ferramenta de Gerenciamento de Serviços de TI (ITSM) do TJCE, a fim de permitir o acompanhamento do histórico do ciclo de vida dos chamados (registro, análise, intervenções e encerramento) abertos pela CONTRATADA e a equipe de segurança da informação do TJCE. A CONTRATADA contará com o devido treinamento da ferramenta de ITSM imediatamente após o início da execução dos serviços e antes dos 30 dias iniciais após assinatura do TRD de implantação.

1.7. Frameworks referenciais: a execução dos serviços prestados, principalmente o processo de resposta a incidentes e testes de invasão ou penetração, devem seguir as boas práticas dos seguintes frameworks: MITRE ATT&CK, NIST, SANS, OSSTMM 3, ISSAF/PTF, ISO 27000 e OWASP.

2. SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA (BLUE TEAM)

2.1. O Blue Team desempenhará um papel fundamental na identificação, investigação e mitigação de incidentes, visando garantir a integridade e disponibilidade dos sistemas de informação. As atividades do Blue Team serão medidas por Níveis Mínimos de Serviço (NMS) e são apresentadas nos itens 2.1 e 2.3.

2.2. Monitoramento de segurança: Os membros do Blue Team devem monitorar continuamente os eventos e incidentes produzidos pelos ativos de redes, sistemas e aplicativos do TJCE (mostrados na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE) em busca de atividades suspeitas. Isso envolve o tratamento de dados gerados pelos Serviços gerenciados de monitoramento e correlação de eventos (SIEM), na sua interação com as ferramentas de segurança já implementadas ou que serão implementadas no TJCE, com o objetivo de identificar eventos ou incidentes de segurança da informação. No entanto, as atividades ou responsabilidades do Blue Team não incluem a administração ou configuração das ferramentas de segurança da informação:

2.2.1. Serviço de Next Generation Firewall (hardware, software e licenças fornecidos pelo TJCE).

2.2.2. Serviço de Web Application Firewall (hardware, software e licenças fornecidos pelo TJCE).

2.2.3. Serviço de VPN – Redes Privadas Virtuais (hardware, software e licenças fornecidos pelo TJCE).

2.2.4. Serviço de Antivírus Corporativo – EDR (software e licenças fornecidos pelo TJCE).

2.2.5. Gestor de Vulnerabilidades (software e licenças fornecidos pelo TJCE).

2.2.6. Ferramenta de Multifactor Authentication - MFA (software e licenças fornecidos pelo TJCE).

2.2.7. Ferramentas, exclusivamente de segurança da informação, a serem implantadas no TJCE.

2.3. Detecção e resposta a incidentes: ao identificar atividades maliciosas ou intrusões, os membros do Blue Team tomam medidas imediatas para responder a esses incidentes. Eles devem analisar e investigar as ameaças, identificar a origem, determinar o escopo do incidente, diagnosticar remediações e acompanhar a aplicação de contramedidas para mitigar os riscos e minimizar o impacto dos ataques.

2.3.1. Análise de segurança: os membros do Blue Team devem analisar regularmente as informações de segurança coletadas de várias fontes, como logs de eventos, alertas de segurança e inteligência de ameaças. Eles devem correlacionar dados e realizar

análises para identificar padrões, tendências e indicadores de comprometimento, ajudando a antecipar e prevenir futuros ataques.

2.3.2. Análise de ameaças: uma vez que uma atividade suspeita é identificada, os membros do Blue Team devem conduzir uma análise de ameaças para determinar a natureza e a gravidade da ameaça. Isso envolve a análise de indicadores de comprometimento (IOCs), como endereços IP, nomes de domínio, logs de eventos, registros de rede e arquivos maliciosos. A CONTRATADA deverá centralizar as ações de correção de segurança na ferramenta SIEM para classificação de prioridade de incidentes e gerenciamento de vulnerabilidades e riscos, usando integração nativa e centralizada com a ferramenta Tenable.

2.3.3. Gerenciamento de vulnerabilidades: será responsabilidade do Blue Team realizar avaliações regulares de vulnerabilidades nos sistemas do TJCE e recomendar as medidas necessárias para mitigar essas vulnerabilidades. Eles também devem acompanhar as atualizações de segurança, patches e correções fornecidas pelos fornecedores de software e hardware, assim como demandar e supervisionar que essas atualizações sejam implementadas.

2.3.4. Coleta de inteligência de ameaças: Os membros do Blue Team devem monitorar ativamente as informações e inteligência de ameaças provenientes de várias fontes, como comunidades de segurança, fornecedores de segurança e agências de inteligência. Esses dados ajudam a identificar novas tendências de ameaças, táticas e técnicas utilizadas pelos atacantes, permitindo que o SOC esteja preparado e atualizado para enfrentar essas ameaças.

2.3.5. Desenvolvimento de políticas de segurança: os membros do Blue Team devem ser responsáveis por avaliar, modificar e desenvolver políticas, normas e procedimentos de segurança (existentes ou novos) que ajudem a proteger os sistemas e a infraestrutura do TJCE. Isso deve incluir a definição de requisitos de segurança para novos projetos, a aplicação de controles de acesso e a criação de políticas de senhas.

2.3.6. Monitoramento de conformidade: o Blue Team é responsável por demandar que as políticas, padrões e regulamentações de segurança sejam seguidos dentro do TJCE. O Blue Team deve monitorar e relatar violações de conformidade, demandar a aplicação de medidas corretivas e conferir que os sistemas e processos estejam alinhados com as diretrizes de segurança do TJCE.

2.3.7. Auditorias de Segurança Internas: avaliação sistemática das políticas, normas, procedimentos e controles de segurança existentes, por meio de revisões de controles,

verificação da conformidade, identificação de lacunas e elaboração de relatórios detalhados com recomendações para melhoria e planos de ação corretiva.

2.3.8. Auditorias de segurança externas: avaliar a postura de segurança do TJCE, definindo escopo, gerenciando o processo de auditoria, revisando relatórios, implementando recomendações e acompanhando o progresso das ações corretivas, visando garantir a conformidade, identificar vulnerabilidades e fortalecer as medidas de segurança.

2.3.9. Avaliação de riscos: avaliar os riscos associados às vulnerabilidades identificadas durante os testes de penetração (ver item 3). Classificar as vulnerabilidades com base em sua gravidade, impacto potencial e probabilidade de exploração, fornecendo informações importantes para a priorização de ações corretivas.

2.3.10. Recomendações de segurança: com base nos resultados das avaliações de segurança, devem ser fornecidas recomendações detalhadas para fortalecer as defesas do TJCE com indicações de atualizações de software, configurações de segurança, políticas e práticas recomendadas para mitigar as vulnerabilidades identificadas. A CONTRATADA abrirá as Requisições de Serviço contendo as recomendações de correções, acompanhará e validará a execução das recomendações, as quais serão executadas pela equipe do TJCE.

2.3.11. Colaborar com a equipe de Red Team e outras equipes de segurança para identificar pontos fracos, testar a eficácia das medidas de segurança e recomendar melhorias.

2.3.12. Treinamento: a contratada deverá, a cada 2 meses, realizar apresentação remota via Microsoft Teams do próprio TJCE, para os servidores do TJCE sobre conscientização em Segurança da Informação com duração mínima de 1 hora. Previamente deverá apresentar o plano da apresentação (roteiro do treinamento e material didático utilizado) para aprovação pela equipe de segurança do TJCE. A divulgação, agendamento e emissão dos certificados de participação ficará a cargo do TJCE/SETIN/Assessoria de Comunicação. O TJCE realizará a gravação do treinamento e a CONTRATADA deverá concordar na cessão de direitos de uso de material didático, assim como da voz, imagem e vídeo do instrutor e do material didático apresentado.

2.3.13. Resposta a incidentes: em caso de incidentes de segurança de níveis médios ou grave, ou emergências cibernéticas, os membros do Blue Team devem atuar como parte principal integrante da equipe de resposta a incidentes. Isso envolve o diagnóstico do incidente e a demanda de contramedidas imediatas para conter a propagação de ataques, isolamento de sistemas afetados, remoção de malware, restauração de

backups e outras ações para mitigar os danos causados pelo incidente. O Blue Team deve coordenar e colaborar com outras equipes envolvidas na resposta, como a equipe de TI, a equipe de comunicações e outras partes interessadas, para restaurar a segurança e a normalidade das operações governamentais. Os seguintes processos de resposta a incidentes, ou variações em função de Frameworks de segurança da informação, devem ser seguidos:

2.3.13.1. O processo de resposta a incidentes de segurança será iniciado sempre que um evento adverso for relatado pelo Serviço Gerenciado de Monitoramento e Correlação de Eventos (conforme descrito neste Anexo), mas não se limitando exclusivamente a ele.

2.3.13.2. Após a abertura do incidente de segurança, cabe ao Blue Team, com o apoio de outros profissionais de TI do TJCE, analisar os logs e artefatos enviados, visando identificar inicialmente as fontes responsáveis pela geração desses logs.

2.3.13.3. Após a realização das análises iniciais do incidente, o Blue Team deverá empenhar-se na identificação dos principais vetores de ataque que comprometeram o ambiente do TJCE.

2.3.13.4. Como próximo passo, o Blue Team deverá informar ao time de segurança da informação do TJCE, seguindo os Níveis Mínimos de Serviços descritos neste documento, as informações preliminares sobre o incidente de segurança ocorrido, juntamente com as estratégias e abordagens planejadas para resolver o incidente. O Blue Team deve fornecer dados e informações mínimas esperadas, conforme especificado a seguir:

2.3.13.4.1. Prioridade: o incidente será representado por um número que indicará sua prioridade ou severidade, em uma escala de 1 a 4, sendo 1 a prioridade mais alta.

2.3.13.4.2. Classificação: deverá ser atribuída uma única palavra que classifique o tipo do incidente, como malware, phishing, misconfiguration, entre outros.

2.3.13.4.3. Fonte do incidente: devem ser fornecidos os detalhes dos nomes dos dispositivos, endereços de e-mail, endereços IP, detalhes da vulnerabilidade ou outros elementos de identificação que indiquem a origem do incidente.

2.3.13.4.4. Destino do incidente: Deve ser fornecidos os detalhes dos

nomes dos dispositivos, endereços de e-mail, endereços IP ou outros elementos de identificação que indicam os ativos afetados.

2.3.13.4.5. Ações recomendadas: devem ser fornecidas instruções inteligentes e de fácil compreensão, que detalhem as ações de remediação já realizadas pelo Blue Team, assim como as ações que o TJCE deve tomar.

2.3.13.4.6. Fontes da Detecção: devem ser fornecidos os detalhes das fontes dos logs ou dos dispositivos de segurança que identificaram (ou colaboraram na identificação) do incidente. Essa informação será útil para análise da causa raiz ou para a implementação de medidas de remediação direcionadas.

2.3.13.5. Em conjunto com o TJCE, o Blue Team será responsável por determinar a severidade do incidente de segurança. A severidade do incidente de segurança da informação será estabelecida levando em consideração a combinação de urgência e impacto, sendo que o impacto representa a crítica do incidente em relação aos aspectos do negócio, e a urgência refere-se à velocidade necessária para sua resolução.

2.3.13.6. Após as análises iniciais do incidente, será responsabilidade do Blue Team realizar uma análise mais aprofundada, levando em consideração o comportamento do ataque e/ou artefato (por exemplo: malware).

2.3.13.7. Após a identificação do comportamento e dos principais vetores de ataque, o Blue Team deverá elaborar uma estratégia para a mitigação e contenção do ataque em questão. No caso de ser necessário realizar alterações no ambiente computacional do TJCE para conter e mitigar o incidente, tais alterações devem ser autorizadas previamente e implementadas pelo corpo técnico de segurança do TJCE. Após a obtenção da autorização, a equipe de segurança do TJCE poderá implementar as alterações necessárias.

2.3.13.8. Após a mitigação do incidente de segurança, o próximo passo exigido é que o Blue Team inicie o processo de coleta de todas as evidências relevantes e identifique os serviços afetados. Essas evidências serão utilizadas ao longo do processo, visando a realização da análise forense do caso.

2.3.13.9. O processo de restauração dos serviços e soluções afetadas será

acompanhado pelo Blue Team e será realizado pela equipe de segurança da informação e de tecnologia da informação do TJCE.

2.3.13.10. O Blue Team deve consolidar os dados coletados durante o processo de tratamento do incidente, a fim de iniciar a análise forense correspondente. Essa análise tem como objetivo identificar pessoas, locais e/ou eventos relevantes, correlacionando todas as informações coletadas e gerando um laudo final sobre o incidente de segurança em questão.

2.3.13.11. O Blue Team é responsável por conduzir a reconstrução dos ataques em todos os incidentes que resultaram em invasão ou vazamento, ou quando considerado necessário, em um ambiente controlado, como sandbox em servidores físicos, máquinas virtuais, ferramentas em nuvem ou outros ambientes computacionais. Esse ambiente deve ser implementado, controlado e de propriedade da CONTRATADA.

2.3.13.12. É incumbência do Blue Team documentar as lições aprendidas do incidente de segurança em questão, ao longo de todo o período de vigência do contrato, com o intuito de construir uma extensa base de conhecimento sobre ataques adversos.

2.3.13.13. O processo descrito é o mínimo esperado a ser seguido e executado pelo Blue Team, no entanto, devido ao caráter contínuo do serviço estabelecido neste Anexo, espera-se que o Blue Team busque constantemente melhorias, as quais podem ser implementadas mediante aprovação do TJCE.

2.4. Perfil do BlueTeam.

2.4.1. Todos os profissionais do Blue Team devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS ou contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 18 meses.

2.4.2. Perfil do Especialista em Segurança - Coordenador do SOC.

2.4.2.1. Será o responsável por gerenciar os profissionais do Blue Team, Red Team e do Serviço de monitoramento e correlação de eventos.

2.4.2.2. Será líder e parte da equipe Blue Team (ver Tabela 2. Força de Trabalho Orientativa).

2.4.2.3. Deve contar com a certificação Certified Information Systems Security Professional (CISSP).

2.4.2.4. Deve contar, ou obter em no máximo 6 meses após a contratação, com

pelo menos, uma das seguintes certificações: Certified Information Systems Auditor (CISA); Certified Information Security Manager (CISM); GIAC Security Essentials Certification (GSEC); Certified Incident Handler (GCIH); CompTIA CySA+.

2.4.3. Perfil do Analista de Segurança Pleno - Blue Team.

3. Deve contar com, pelo menos, uma das seguintes certificações: Certified Information Systems Auditor (CISA); Certified Incident Handler (GCIH); CompTIA CySA+.**SERVIÇO DE GESTÃO TESTES DE INVASÃO (RED TEAM)**

3.1. O Red Team será responsável por conduzir avaliações de segurança e testes de penetração, internos e externos, nos sistemas, aplicativos e infraestrutura do TJCE, com o objetivo de identificar vulnerabilidades e avaliar a eficácia das medidas de segurança implementadas.

3.2. O Red Team trabalhará em estreita colaboração com a equipe de segurança da informação, fornecendo *insights* e recomendações para melhorar a postura de segurança do órgão.

3.3. Responsabilidades ou atividades do Red Team.

3.3.1. Testes de invasão: realizar testes de penetração simulando ataques cibernéticos para identificar vulnerabilidades nos sistemas, redes e aplicativos do TJCE. Explorar técnicas avançadas de hacking ético para encontrar pontos fracos na segurança e avaliar a eficácia das defesas existentes.

3.3.2. Os alvos dos testes de invasão, assim como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados pela equipe de segurança da informação do TJCE, mediante Requisição de Serviço disponibilizado através da ferramenta de ITSM do TJCE, antes de cada campanha a ser executada.

3.3.3. Qualquer atividade que possa comprometer ou prejudicar um ambiente ou ativo do TJCE deve ser comunicada imediatamente, antes de sua execução, devido à importância de manter a disponibilidade dos ambientes e serviços em funcionamento.

3.3.4. As seguintes ferramentas tecnológicas devem contar com licenciamento e ser disponibilizadas pela CONTRATADA para o uso do Red Team nos testes de invasão, sob demanda das atividades do TJCE para o Red Team (qualquer dúvida ou questionamento de dimensionamento deve ser realizado na Vistoria Técnica):

3.3.4.1. Metasploit Pro.

3.3.4.2. Shodan.

3.3.4.3. Burp Suite Professional.

3.3.4.4. DeHashed.

.

3.3.5. O teste de invasão deverá obedecer às seguintes fases, podendo ser adaptadas conforme os Frameworks existentes na literatura:

3.3.5.1. Planejamento.

3.3.5.1.1. Na fase de planejamento, todas as premissas, processos, atividades e cronogramas descritos e aprovados na Requisição de Serviço

serão detalhados e apresentados.

3.3.5.1.2. Serão fornecidas informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser aplicadas ambas, de acordo com a definição do escopo):

3.3.5.1.2.1. Técnica da caixa-preta: envolve ter pouco ou nenhum conhecimento prévio sobre o ambiente a ser avaliado. O especialista em segurança deverá descobrir e explorar o ambiente durante o processo de avaliação.

3.3.5.1.2.2. Técnica da caixa branca: permite que o avaliador tenha acesso irrestrito a todas as informações relevantes para o teste de segurança.

3.3.5.1.2.3. Técnica da caixa cinza ou híbrida: o avaliador tem conhecimento limitado sobre o alvo, ou seja, uma média de informações e recursos disponíveis entre as técnicas de caixa preta e branca.

3.3.5.2. Descoberta

3.3.5.2.1. Deverá ser utilizada, no mínimo, ferramentas de análise de vulnerabilidades, bem como a gestão de vulnerabilidades, além de empregar técnicas manuais de análise de vulnerabilidade. As ferramentas devem ser apresentadas para conhecimento e aprovação prévia antes de sua utilização, assim como a metodologia empregada na análise manual de vulnerabilidades.

3.3.5.2.2. Durante a fase de Descoberta, os seguintes requisitos devem ser cumpridos e incluídos no "Relatório de Teste de Invasão", quando aplicável:

1. Coleta passiva, com a utilização de, no mínimo, as seguintes técnicas: Whois e nslookup (consultas DNS) ; Sites de busca; Listas de discussão; Blogs de colaboradores; Dumpster diving ou trashing; Informações livres; Packet sniffing “passive eavesdropping”; Captura de banner.
2. Coleta ativa, com a utilização de, no mínimo, as seguintes técnicas: Port scanning (Mapeamento de rede);

Varredura de vulnerabilidade.

3. Varredura de vulnerabilidade para identificar: Hosts ativos na rede; Portas e serviços em execução; Serviços ativos e vulneráveis nos hosts; Sistemas operacionais; Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas; Configurações feitas nos hosts sem observância de boas práticas em segurança computacional; Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas; Identificação de vetores de ataque e cenários para exploração; Vulnerabilidades Detectadas (CVE); Vulnerabilidades de Alto Risco; Vulnerabilidades de Médio Risco; Vulnerabilidades de Baixo Risco; Informações a serem aplicadas na fase de ataques.
4. Análise de serviços e aplicações web: Uso indevido de sistema de arquivos e arquivos temporários; Evasão de informação por configurações default de tratamento de erros; Tratamento indevido de entrada; Problemas relacionados à má configuração dos serviços; Gerenciamento inseguro de sessões web.

3.3.5.3. Ataque

3.3.5.3.1. Todas as atividades suspeitas de comprometer um ambiente ou ativo devem ser relatadas imediatamente antes de sua execução, levando em consideração a importância de manter a disponibilidade dos ambientes e serviços em funcionamento.

3.3.5.3.2. Deverá ser conduzido um teste de vulnerabilidades e invasão em endereços IPs, URLs, aplicações ou outros ativos especificados do ambiente computacional, incluindo servidores, bancos de dados, ativos de rede, equipamentos de segurança e outros dispositivos relevantes para o teste de invasão.

3.3.5.3.3. Deverão ser aplicados, no mínimo, os seguintes tipos de ataques: Violações do protocolo HTTP; SQL Injection; LDAP Injection;

Cookie Tampering; CrossSite; Scripting (XSS); Directory Transversal; Buffer Overflow; OS Command Execution; Command Injection;nRemote Code Inclusion; Server Side Includes (SSI) Injection; File disclosure; Information Leak; Zero day attacks; DDos (Distribuited Denial of Service); Dos (Denial of Service); Contra protocolo TCP; Ataques contra a aplicação e OWASP Top 10.

3.3.5.3.4. Os ataques de negação de serviço, tanto no protocolo TCP quanto no nível de aplicação, devem utilizar/demonstrar/explorar, no mínimo, as seguintes técnicas específicas: Bugs em serviços, aplicativos e sistemas operacionais; SYN flooding; Fragmentação de pacotes de IP (Smurf e fraggle, Teardrop, nuke e land); Ataques contra o protocolo TCP (Sequestro de conexões; Prognóstico de número de sequência do protocolo TCP; Ataque de Mitnick; Source routing).

3.3.5.3.5. Ataques em nível da aplicação: Buffer Overflow; Problemas com o SNMP; Vírus, worms e cavalos de Tróia.

3.3.5.3.6. Ataques de injeção de Código: Ataques XSS (Crosssite Script); Comprometimento do acesso remoto; Manutenção de acesso; Encobrimento de rastros da invasão.

3.3.5.3.7. Para os testes de invasão direcionados aos serviços web, abrangendo tanto a Intranet quanto a Internet, serão considerados e aplicados os seguintes testes com base no OWASP TESTING GUIDE 4.2:

1. Padrões para testes de gerenciamento de configuração: OWASPCM001, OWASPCM002, OWASPCM003, OWASPCM004, OWASPCM005, OWASPCM006, OWASPCM007, OWASPCM008.
2. Padrões para testes de autenticação: OWASPAT001, OWASPAT002, OWASPAT003, OWASPAT004, OWASPAT005, OWASPAT006, OWASPAT007, OWASPAT008, OWASPAT009 e

OWASPAT010.

3. Padrões para testes de gerenciamento de sessão: OWASPSM001, OWASPSM001, OWASPSM002, OWASPSM003, OWASPSM004, OWASPSM005.
4. Padrões para testes de autorização: OWASPAZ001, OWASPAZ002 e OWASPAZ003.
5. Padrão para testes de negócio lógico: OWASPBL001.
6. Padrões para testes de validação de dados: OWASPDV001; OWASPDV002, OWASPDV003, OWASPDV004, OWASPDV005, OWASPDV006, OWASPDV007, OWASPDV008, OWASPDV009, OWASPDV010, OWASPDV011, OWASPDV012, OWASPDV013, OWASPDV014, OWASPDV015 e OWASPDV016.
7. Padrões para testes de negação de serviços: OWASPDS001, OWASPDS002, OWASPDS003, OWASPDS004, OWASPDS005, OWASPDS006, OWASPDS007 e OWASPDS008.
8. Padrões para testes de serviços web: OWASPWS001, OWASPWS002, OWASPWS003, OWASPWS004, OWASPWS005, OWASPWS006 e OWASPWS007.

3.3.5.3.8. Cada teste realizado deve ser acompanhado por relatórios que incluam os seguintes resultados: Referência-base (Whitepaper); Ameaças encontradas; Riscos levantados ao ambiente computacional; Contramedidas para mitigar as ameaças encontradas.

3.3.5.4. Relatório de Teste de Invasão

3.3.5.4.1. Após a conclusão da fase de ataque, será elaborado e entregue à equipe de segurança do TJCE um relatório de Teste de Invasão,

abrangendo cada teste realizado e contendo, no mínimo, as seguintes informações: objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão.

3.3.5.4.2. Ao final da fase de ataque, no Relatório de Teste de Invasão, devem ser abordadas e detalhadas, no mínimo, as seguintes informações: Detalhes da infraestrutura descoberta, alvo dos testes de invasão; Equipamentos e recursos demandados para este teste; Tipos de ataque; Prazos (janelas de tempo para execução dos testes); Pontos de contato da CONTRATADA (responsáveis para tratamento de questões abordadas nos testes); Tipos de testes realizados pelos especialistas em segurança da informação; Confirmação ou refutação de a existência de vulnerabilidades; Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade; Obtenção de acesso e possível escalada de privilégios; Detalhamento da metodologia do ataque; Recomendações para sanar riscos e vulnerabilidades.

3.3.5.4.3. Uma reunião será realizada entre o Red Team e a equipe de segurança do TJCE, na qual o conteúdo completo do Relatório Teste de Invasão será apresentado detalhadamente. Durante a reunião, todas as dúvidas do corpo técnico do TJCE serão esclarecidas.

3.3.5.4.4. Após a entrega do Relatório Teste de Invasão, o Blue Team, em colaboração com a equipe de segurança do TJCE, procederá à análise do documento com o intuito de implementar as recomendações, mitigar os riscos identificados ou, quando

necessário, aceitá-los.

3.3.5.4.5. Após a análise e implementação das medidas de remediação, a equipe de segurança do TJCE tem a opção de solicitar ao Red Team a realização de um novo teste de invasão para avaliar os resultados, resultando na emissão de um relatório atualizado.

3.3.5.4.6. O prazo para conclusão de cada Requisição de Serviço, que inclui diagnósticos, análises, avaliações e testes, acompanhado da entrega de todos os relatórios específicos de avaliação de vulnerabilidades dos ambientes mencionados neste Anexo, será determinado individualmente para cada atividade, dividindo-se em: Atividades do Pentest; Entrega do relatório "Teste de Invasão"; Ações corretivas das vulnerabilidades apontadas pelo Red Team e aplicadas pelo Blue Team; Reavaliação Pentest, caso necessário; Entrega do Relatório Final do Teste de Invasão. Todas as fases dos testes de invasão devem ser detalhadamente documentadas com evidências na ferramenta de ITSM do TJCE.

3.4. Perfil do Analista de Segurança Sênior - Red Team

3.4.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS ou contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 18 meses.

3.4.2. Deve contar com a certificação Certified Ethical Hacker (CEH).

3.4.3. Deve contar, ou obter em no máximo 6 meses após a contratação, com pelo menos, uma das seguintes certificações: GIAC Exploit Researcher and Advanced Penetration Tester (GXPN); Offensive Security Certified Professional (OSCP); EC-Concil Licensed Penetration Tester (LPT); IACRB Certified Expert Penetration Tester (CEPT); CompTIA Pentest+.

4. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

4.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TJCE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em Frameworks de gestão de incidentes (NIST SP 800-61, ISO/IEC 27035 e SANS Incident Handling) e fornecendo como serviço a solução tecnológica *Security Information and Event Management* (SIEM)

4.2. Características gerais da solução SIEM

4.2.1. A CONTRATADA deve fornecer o serviço de coleta, análise e correlação de logs, por meio de uma solução de Gerenciamento de Informações e Eventos de Segurança (SIEM).

4.2.2. A tecnologia de SIEM a ser implantada deve ter sido homologada e utilizada em outras instituições públicas ou privadas, conforme os documentos de qualificação técnica a serem apresentados pela licitante.

4.2.3. Todo hardware e software deve ser fornecido pela CONTRATADA como serviço na vigência do contrato.

4.2.4. A CONTRATADA deverá implantar coletores (virtualizados ou em hardware) no ambiente do TJCE, a fim de realizar a coleta de logs localmente no ambiente do TJCE, absorvendo toda a responsabilidade de implantação dos coletores (Servidores, Máquinas Virtuais, Processamento, Sistema Operacional, etc). O TJCE somente fornecerá energia e link de conexão para o funcionamento da implantação dos coletores.

4.2.5. Para a implantação dos coletores, poderá ser aceito o uso de *Virtual Appliance* da CONTRATADA a ser instalado no ambiente computacional do TJCE, mediante a verificação e aprovação prévias dos requisitos técnicos pela equipe de segurança da informação do TJCE e o atendimento das demais exigências e requisitos apresentados neste Anexo.

4.2.6. O TJCE fornecerá conectividade, espaço físico em Rack e energia elétrica para o funcionamento do hardware e software da solução SaaS (Software as a Service).

4.2.7. A solução deverá consolidar eventos de log de dispositivos, terminais e aplicativos distribuídos.

4.2.8. A solução deverá correlacionar as informações de diferentes fontes de logs e agregar eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes.

4.2.9. A solução do processamento de dados transmitidos pelos coletores e executada pela ferramenta SIEM deve ser implementada no modelo totalmente SaaS.

4.2.10. A solução deverá ter disponibilidade mensal mínima de 99,7%, conforme Nível Mínimo de Serviço apresentado na Tabela 4. Indicadores de Nível de Serviço.

4.2.11. A solução deve ser flexível a períodos de sazonalidade, permitindo aumento da licença quando necessário e retorno ao volume inicial contratado quando o período de sazonalidade finalizar.

4.2.11.1. A solução deve possibilitar a recepção de eventos que temporariamente

ultrapassem os limites contratados. O volume excedente será processado assim que o volume for normalizado, funcionando com picos temporários sem perder eventos ou incorrer em cobranças adicionais por excesso.

4.2.11.2. A cobrança sobre o volume sazonal será realizada conforme o volume de Eventos por Segundo (EPS) tratado.

4.2.12. A solução deverá possibilitar a coleta dos logs *on-premise*, por meio do uso de agentes.

4.2.12.1. Os agentes devem ser capazes de realizar o monitoramento da integridade de arquivos, alertando sobre inclusão, alteração, remoção e leitura de arquivos presentes em equipamentos Windows/Linux monitorados.

4.2.12.2. Os agentes de coleta devem oferecer suporte para a coleta de logs via Syslog de outras plataformas.

4.2.12.3. Os agentes de coleta devem ser capazes de identificar e separar "relay logs" (servidores Syslog que recebem e repassam logs de várias outras fontes) de forma independente, garantindo uma correlação adequada.

4.2.12.4. A solução deve permitir o monitoramento e envio de alertas relativos a agentes que não estejam funcionando corretamente ou estejam inoperantes.

4.2.12.5. A solução deve operar usando agentes, com exceção dos dispositivos que geram logs usando o protocolo padrão Syslog.

4.2.13. A solução deve disponibilizar o uso da ferramenta *User Behavior Analytics* (UBA) em computadores de usuários determinados pelo TJCE, sem custo adicional e com regras pré-definidas e modificáveis.

4.2.14. Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM.

4.2.15. Quando coletando logs que estão hospedados na nuvem, a coleta deve ocorrer diretamente da nuvem da aplicação para a nuvem do SIEM, sem permitir que os logs passem pela infraestrutura do TJCE. Isso é válido desde que a solução em nuvem permita a coleta por meio de integrações via API. Qualquer questionamento de serviços em nuvem usados pelo TJCE poderão ser esclarecidos na Vistoria Técnica.

4.2.16. A solução deverá segregar logicamente os logs do TJCE dos demais logs de outras contratantes que utilizem a solução de SIEM SaaS na infraestrutura da CONTRATADA.

4.2.17. A solução deve ser monitorada para garantir disponibilidade e infraestrutura em tempo integral, 24 horas por dia, 7 dias por semana, durante todo o ano.

4.2.18. Se a solução consistir em módulos, eles devem ser fornecidos por um único fabricante para garantir suporte completo em relação a funcionalidades, integrações e compatibilidade de 100% com a solução. Como um dos requisitos da ferramenta SIEM para a assinatura do TRD de implantação, a CONTRATADA deverá apresentar documentação fornecida pelo fabricante para comprovar a cobertura de garantia do fabricante relacionada com a funcionalidade da ferramenta SIEM.

4.2.19. A solução deve armazenar os logs por pelo menos 6 meses online, conforme diretrizes da PORTARIA No 162, DE 10 DE JUNHO DE 2021 do CNJ.

4.2.20. O armazenamento dos logs deve ser efetuado no território brasileiro pela CONTRATADA. Os logs não poderão trafegar por território fora do Brasil.

4.2.21. A coleta, normalização e correlacionamento dos eventos dos dispositivos monitorados devem ocorrer em tempo próximo ao real.

4.2.22. A fim de aprimorar a operação e a compreensão dos eventos, é obrigatório normalizá-los e categorizá-los em um único padrão que será utilizado pela solução.

4.2.23. A solução deve possibilitar a criação de metadados personalizados, permitindo a extração de dados existentes na linha de log (raw). Isso pode ser realizado por meio de recursos como expressões regulares ou interfaces gráficas dedicadas para essa finalidade.

4.2.24. Propriedades customizadas poderão ser utilizadas em regras de correlação online e histórica.

4.2.25. A solução deve possibilitar a agregação de eventos similares.

4.2.26. A solução deve atribuir uma métrica de prioridade tanto para os eventos quanto para os alertas/incidentes.

4.2.27. A solução deve ser capaz de gerar alertas/incidentes com base em regras predefinidas anteriormente.

4.2.28. A solução deve ter a capacidade de armazenar os eventos, incluindo aqueles normalizados, de forma compactada.

4.2.29. A solução deve possibilitar a análise de eventos com base em contexto, como usuários, localização geográfica e qualquer outro metadado presente nos eventos.

4.2.30. A solução deve fornecer painéis gráficos ou integração com painéis gráficos existentes no TJCE (dashboards), que apresentam indicadores de segurança, aplicações e monitoramento do SIEM.

4.2.31. Os painéis gráficos (dashboards) devem ser personalizáveis por usuário, permitindo a visualização dos eventos relacionados a um alerta e/ou incidente de segurança

identificado pelas regras de correlação da solução na interface web.

4.2.32. O Dashboard integrado deve:

4.2.32.1. Fornecer um painel que apresente uma visão consolidada das métricas de segurança dos ativos monitorados.

4.2.32.2. Permitir a personalização do painel, incluindo a adição de relatórios e métricas.

4.2.32.3. Realizar a análise dos eventos de segurança da informação em quase tempo real.

4.2.32.4. Assegurar a funcionalidade de análise por meio do drill-down, possibilitando a exploração detalhada a partir de um gráfico de visão geral, com a capacidade de descer aos diferentes níveis de análise conforme necessário.

4.2.32.5. Permitir o acesso da equipe do TJCE em qualquer momento.

4.2.33. Ter a capacidade de enviar e-mails ou mensagens via SMS contendo notificações sobre incidentes ou alertas.

4.2.34. A solução deve oferecer, no mínimo, os seguintes métodos de coleta de eventos: Syslog (UDP, TCP), Syslog com criptografia TLS, JDBC, SNMP (v1, v2 e v3), Registro de Eventos do Microsoft, Cliente MQ Series, Arquivos de Log em formato de texto, Kafka, Checkpoint OPSEC/LEA, CISCO NSEL e Protocolo Juniper NSM.

4.2.35. A solução deve ser capaz de encaminhar os logs e fluxos, em seu formato nativo, para outros sistemas de segurança da informação ou servidores Linux/Windows em tempo real.

4.2.36. A solução deve ser capaz de encaminhar eventos já normalizados para outros sistemas de correlação em tempo real.

4.2.37. A solução deve oferecer a capacidade de configurar a ofuscação de qualquer parte dos dados recebidos após a normalização. A configuração da ofuscação de dados deve ser realizada por meio de chaves de criptografia.

4.2.38. A solução deve ser capaz de automatizar a resposta a incidentes, executando scripts como ação personalizada dentro das regras de correlação.

4.2.39. A solução deve permitir a personalização e customização de diversos modelos de e-mail que serão enviados como resposta aos incidentes identificados.

4.2.40. A solução deve ser capaz de processar logs no formato JSON, identificando e criando automaticamente os campos comuns do log como metadados para aquele tipo de log.

4.2.41. A solução deve permitir a criação de metadados com nomes personalizados, à escolha

do administrador, e possibilitar a referência desses metadados em pesquisas e regras de correlação.

4.2.42. A solução deve permitir a personalização/definição de metadados para extrair dados de uma linha de log (raw), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, possibilitando o uso desses dados em pesquisas de eventos.

4.3. Características do coletor de logs do SIEM

4.3.1. A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de preferência (network appliance ou virtualização), desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos do TJCE.

4.3.2. Os coletores deverão comunicar-se com o SIEM da CONTRATADA através de VPN com tráfego criptografado.

4.3.3. Deverá possibilitar a compressão/compactação e criptografia dos dados para o envio dos logs à nuvem.

4.3.4. Deverá realizar a filtragem e seleção dos eventos a serem inseridos na solução ou mantidos na base de dados da solução, conforme períodos definidos previamente.

4.3.5. Deverá possibilitar a criação e modificação de políticas de retenção.

4.3.6. Deverá realizar a normalização e categorização dos eventos em um padrão único, que será utilizado pela solução.

4.3.7. Deverá oferecer suporte nativo para o reconhecimento e coleta de pelo menos 250 tipos distintos de fontes de dados.

4.3.8. Deverá processar eventos em formato comprimido (zip, gz, tar.gz) sem exigir descompressão manual.

4.3.9. Deverá realizar a agregação de eventos, exibindo a contagem de ocorrências quando o mesmo evento acontecer dentro de um período curto.

4.3.10. A possibilidade de efetuar a agregação de eventos deve ser configurável, permitindo escolher entre realizar ou não essa operação.

4.3.11. Deverá preservar o evento bruto (raw), juntamente com seus metadados para fins de armazenamento e consultas futuras.

4.3.12. Deverá ter a capacidade de agregar informações de localização geográfica dos endereços IP envolvidos no evento, a fim de utilizá-las na correlação.

4.3.13. Um único componente da solução deve ter a capacidade de coletar, processar e normalizar tanto os eventos de segurança quanto os eventos de negócio (não

relacionados à segurança).

4.3.14. Os eventos de segurança e de negócios devem ser normalizados para um único padrão de eventos.

4.3.15. A solução deve oferecer suporte à integração de dispositivos ou logs que não são nativamente suportados.

4.3.16. A integração de logs ou dispositivos deve ser feita através da interface web, utilizando expressões regulares, JSON e recursos similares, sem definir de maneira obrigatória a utilização de linguagens de programação ou scripts, como Java, C, TCL/TK, PowerShell, Shell Scripts, entre outros.

4.3.17. A integração mencionada deve ser compatível com as seguintes formas de coleta de eventos:

4.3.17.1. Check Point OPSEC/LEA.

4.3.17.2. Kafka.

4.3.17.3. Arquivos de Log em Formato de texto.

4.3.17.4. Syslog (UDP, TCP).

4.3.17.5. Microsoft Event Log.

4.3.17.6. Juniper NSM Protocol.

4.3.17.7. SNMP (v1, v2 e v3).

4.3.17.8. CISCO NSEL.

4.3.17.9. Syslog criptografado com TLS.

4.3.17.10. PAN-OS XML

4.3.17.11. Common Event Format (CEF)

4.3.17.12. Outros formatos de logs presente nos ativos de rede do TJCE (switches, access point, etc).

4.3.18. A solução precisa ter suporte incorporado para, no mínimo, as seguintes fontes de logs:

4.3.18.1. Windows.

4.3.18.2. Linux.

4.3.18.3. IBM/AIX.

4.3.18.4. HP-UX, Solaris.

4.3.18.5. Oracle Database.

4.3.18.6. IBM/DB2.

4.3.18.7. PostgreSQL.

4.3.18.8. MS SQL Server.

4.3.18.9. Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet, Hillstone, Huawei, Palo Alto e SonicWall).

4.3.18.10. Network IPS/IDS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee).

4.3.18.11. Outras fontes de logs de tecnologias presentes na infraestrutura do TJCE.

4.3.19. A solução deve oferecer a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, a partir das opções nativamente suportadas e enviadas via Syslog.

4.3.20. A solução deve ter a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, incluindo tipos de logs personalizados na solução, quando enviados via Syslog.

4.3.21. A solução deve ter suporte para IP overlap, ou seja, categorizar os eventos de forma que seja possível gerenciar eventos provenientes de fontes de log que estão em redes distintas, mas possuem o mesmo endereço IP.

4.4. Recursos de correlação de logs do SIEM.

4.4.1. Considera-se tempo de processamento “quase real” no receptor, ao processamento instantâneo da informação mais o atraso de tráfego de dados entre o emissor e o receptor.

4.4.2. A solução deve realizar a correlação de eventos provenientes das fontes de logs e flows, resultando na geração de incidentes de segurança.

4.4.3. A solução deve efetuar a correlação dos eventos em tempo quase real.

4.4.4. A solução deve efetuar a correlação dos flows em tempo quase real.

4.4.5. A solução deve oferecer a capacidade de criar regras inexistentes e editar as existentes.

4.4.6. A solução deve permitir a correlação de qualquer informação presente no evento, inclusive dados financeiros ou outras informações que não estejam relacionadas a endereçamento IP, portas, etc.

4.4.7. Oferecer um mínimo de 150 regras incorporadas, permitindo a criação ilimitada de novas regras ou personalização das regras incorporadas:

4.4.7.1. Ataques de força bruta com e sem sucesso.

4.4.7.2. Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis).

4.4.7.3. Infecção de equipamentos por vírus.

4.4.7.4. Comprometimento ou invasão de ativos da rede.

4.4.7.5. Anomalias de Logon: excessivas falhas de logon, logons fora do expediente,

logons a partir de endereços IP não usuais.

4.4.7.6. Realização de ações suspeitas por parte de usuários privilegiados.

4.4.7.7. Detecção de padrões em logs observados e não observados.

4.4.7.8. Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade).

4.4.7.9. Bloqueio de contas e password scans.

4.4.7.10. Ataques comuns em aplicações WEB, como XSS e SQL injection.

4.4.7.11. Ataques de negação de serviço (DoS e DDoS).

4.4.7.12. Identificação em tempo real e de maneira automatizada da origem dos eventos de segurança, identificando cidades, estados e países e não somente os endereços IP de origem.

4.4.7.13. Botnets, worms, DDoS e outros zero-day malwares, através do cruzamento dos logs de DNS, DHCP, web proxy e tráfego de rede.

4.4.8. As regras podem variar desde a detecção simples de thresholds até o uso de operadores lógicos comuns para correlacionar eventos distintos, possibilitando:

4.4.8.1. Permitir a utilização de thresholds estáticos ou dinâmicos.

4.4.8.2. Facilitar a execução de scripts automáticos em casos de incidentes.

4.4.8.3. Permitir a configuração de políticas de notificação com base na severidade do incidente, hora do dia e serviço.

4.4.8.4. Integrar a solução com a monitoração de capacidade e desempenho dos ativos gerenciados via SNMP.

4.4.9. A capacidade de autodetecção deve incluir:

4.4.9.1. Oferecer recursos mínimos de busca de eventos, incluindo: busca em tempo real utilizando palavras-chave semelhantes ao Google e consultas estruturadas semelhantes ao SQL, assim como ter a capacidade de converter os resultados da busca em relatórios ou widgets de painel.

4.4.10. A solução deve incluir regras de correlação específicas para regulamentações e conformidades aplicáveis ao TJCE, com suporte mínimo para PCI, ISO 27001 e GDPR ou LGPD.

4.4.11. A solução deve possuir um repositório que ofereça novas regras de correlação especializadas em segurança para atualização e expansão da capacidade de detecção de incidentes, sem custos adicionais.

4.4.12. A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surtos ou ausência de eventos/tráfego, quando comparados a

períodos semelhantes (por exemplo, mesmo período do dia, mesmo dia da semana).

4.4.13. A solução deve permitir a criação de regras que identifiquem desvios em qualquer metadado, em relação aos limites preestabelecidos.

4.4.14. A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que ocorrem ao longo do tempo e não foram previstos ou observados anteriormente.

4.4.15. A solução deve integrar-se com ferramentas externas como Nslookup, Whois e Nmap.

4.4.16. A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (watchlist), permitindo também a criação e edição automatizada e manual de listas.

4.4.17. A solução deve ser capaz de correlacionar eventos e fluxos de rede, como NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução.

4.4.18. A solução deve ser capaz de correlacionar eventos provenientes de múltiplas fontes, tipos ou localizações.

4.4.19. A solução deve ter a capacidade de priorizar os eventos e incidentes com base em critérios que incluem, pelo menos, severidade e criticidade/relevância do evento ou incidente. Deve ser possível utilizar uma combinação desses critérios para determinar a prioridade.

4.4.20. Os incidentes devem ser agrupados, no mínimo, de acordo com:

4.4.20.1. Endereço de origem.

4.4.20.2. Endereço de destino.

4.4.20.3. Categoria.

4.4.21. A solução deve ter, no mínimo, os seguintes tipos de correlação:

4.4.21.1. Extrapolação de um limite (threshold).

4.4.21.2. Correlação por anomalia e padrão de comportamento.

4.4.21.3. Correlação por regras.

4.4.22. Como resultado das regras, a solução deve ter a capacidade de realizar ações automáticas, no mínimo:

4.4.22.1. Enviar e-mail.

4.4.22.2. Enviar mensagem para o usuário conectado no console.

4.4.22.3. Criar um incidente no sistema de workflow interno.

4.4.22.4. Enviar traps SNMP e popular listas (watchlist).

4.4.23. A solução deve possuir a capacidade de se integrar com os principais sistemas de

inteligência de ameaças de riscos globais e das soluções de segurança da informação presente no TJCE, tais como: PAN-DB, Tenable.io Threat Intelligenc, Kaspersky Threat Intelligence, HP ThreatLink (DVLabs), Symantec DeepSight, Verisign iDefense, IBM X-Force, etc.

4.4.24. A solução deve oferecer a flexibilidade de utilizar qualquer metadado dos eventos em regras de correlação.

4.4.25. A solução deve permitir testar as regras de correlação em eventos passados, com um período de tempo e escopo claramente definidos.

4.4.26. A correlação histórica deve fornecer a opção de escolher o período a ser analisado, com suporte mínimo para correlação de 1 dia, 7 dias e 30 dias.

4.4.27. As regras de correlação histórica devem processar logs e flows, gerando alertas quando os eventos/flows analisados corresponderem às especificações definidas na regra.

4.4.28. Uma regra de correlação deve ter a capacidade de correlacionar eventos de tipos e origens distintos, verificando situações como a sequência de eventos diferentes, a contagem de eventos e a ausência de um evento após a ocorrência de outro.

4.5. Recursos da console de administração e operação do SIEM.

4.5.1. A console de administração e operação deve ser configurada e operada pela CONTRATADA.

4.5.2. A console de consulta deve incluir a capacidade de classificar os eventos em geral em três grupos distintos:

4.5.2.1. Eventos de auditoria (logins, logouts, erros de autenticação, etc.).

4.5.2.2. Eventos de Segurança (ataques, comprometimento, roubo de dados, fraudes, etc.).

4.5.2.3. Eventos de Operação (erros, eventos críticos de ativos e rede, etc.).

4.5.3. A console deve contar com as seguintes especificações:

4.5.3.1. Ter uma interface web única, via HTTPS, para administração, gerenciamento e operação do sistema como um todo, garantindo a confidencialidade dos dados.

4.5.3.2. Ter acesso controlado e autenticado por usuário.

4.5.3.3. Ter capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários.

4.5.3.4. Permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0.

4.5.3.5. Garantir acesso aos dados e funcionalidades específicas por perfis de usuário.

4.5.3.6. O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução de acordo com os perfis de usuários definidos pelo administrador.

4.5.3.7. O controle de acesso deve ser configurado para permitir o acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, atividades de Redes e Logs.

4.5.3.8. Permitir a visualização de eventos, flows de rede e incidentes de segurança em tempo quase real.

4.5.3.9. Permitir a pesquisa nos eventos históricos com base em metadados, oferecendo a capacidade de drill-down, ou seja, refinamento da pesquisa a partir da seleção de elementos no resultado para realizar uma nova pesquisa.

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

4.5.3.11. A solução deve permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

4.5.3.12. Ter a capacidade de criar novos painéis gráficos (dashboards) e modificar os existentes.

4.5.3.13. Ter a capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (exemplo: Firewall, Proxy e antivírus na mesma visualização).

4.5.3.14. Ter a capacidade de criar listas (watchlist) e alterar as existentes, permitindo a inserção dos dados de forma manual, por linha de comando e automática por meio das regras de correlação.

4.5.3.15. Permitir a remoção de dados das listas (watchlist) de forma manual, automática por meio das regras de correlação e por expiração do tempo de vida da informação.

4.5.3.16. Possuir a capacidade de gerenciar e configurar centralmente todas as partes distribuídas da solução.

4.5.3.17. Possuir a capacidade de atualizar os componentes da solução por meio da console central de administração.

4.5.3.18. Ter a capacidade de restaurar informações de cópia de segurança do banco

de dados, configurações e dados que foram arquivados previamente pela solução.

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

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

4.5.3.21. Para análise dos eventos e flows de rede, é necessário ter suporte a filtros de eventos, incluindo filtros simples, pesquisa de expressões e buscas avançadas diretamente na base de dados.

4.5.3.22. Deve oferecer APIs do tipo webservices, seguindo o padrão "RESTful API", para permitir o acesso externo à solução, possibilitando a busca de informações de eventos e flows, assim como a manipulação de incidentes.

4.5.3.23. Deve suportar o controle de acesso à solução com base em informações externas, validando atributos do usuário ou grupo a que ele pertence. Essa validação de autorização deve ser suportada em diretórios LDAP ou Windows Active Directory.

4.5.3.24. Deve fornecer uma API para a criação de fontes de logs (data sources) por meio de uma interface ReST, com o objetivo de automatização.

4.5.4. Os relatórios devem contar com as seguintes especificações:

4.5.4.1. Deve permitir a geração de relatórios, em quase tempo real, que englobem diversas informações em um único documento, como dados de segurança e rede.

4.5.4.2. Fornecer a funcionalidade de geração de relatórios de conformidade, abrangendo, pelo menos, SOX, PCI e ISO.

4.5.4.3. Deve ser permitido agendar a execução de relatórios em qualquer horário ou período, com a opção de enviar os resultados por e-mail.

4.5.4.4. Deve permitir a criação de relatórios relacionados a incidentes, logs, flows de rede e vulnerabilidades.

4.5.4.5. Deve organizar os relatórios em grupos temáticos, permitindo a criação de novos agrupamentos de relatórios pelos usuários.

4.5.4.6. Deve possibilitar a personalização de novos relatórios com base em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes.

4.5.4.7. Deve gerar relatórios de eventos, alertas/incidentes em níveis técnico e

gerencial, que podem ser exportados nos formatos PDF, HTML, XLS, CSV, XML e RTF/DOC.

4.5.4.8. Os usuários devem ter acesso apenas aos seus próprios relatórios ou aos relatórios disponibilizados por outros usuários. Os administradores devem ter acesso a todos os relatórios.

4.5.4.9. Deve ser possível definir perfis de usuários com permissões/restrições para editar os modelos de relatórios.

4.5.4.10. Deve ser possível gerar relatórios com base em dados que contenham endereços IPv6.

4.5.4.11. A funcionalidade de backup deve preservar os dados dos relatórios.

4.5.4.12. Deve permitir a geração de relatórios que incluam os eventos associados a um incidente detectado por regras de correlação.

4.5.4.13. Permitir classificar eventos de segurança: ataques, reconhecimento, malware, atividades suspeitas de rede ou usuários, etc.

4.5.4.14. Contar com a opção de incluir os TOP endereços lógicos de origem das ameaças, TOP países e cidades de origem das ameaças e dos alertas de segurança.

4.5.5. A CONTRATADA deverá garantir que terá acesso ao suporte do fabricante da tecnologia SIEM durante a vigência do contrato. Para isso, a CONTRATADA deverá apresentar um acordo de suporte direto com o fabricante, assegurando que terá acesso a especialistas qualificados para resolver dúvidas, consultas ou problemas de configuração relacionados à ferramenta SIEM.

4.6. Dimensionamento do SIEM.

4.6.1. Considerando os elementos listados na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE as seguintes ferramentas consultadas:

4.6.1.1. Planilha de cálculo de EPS da IBM baseada no preenchimento na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE, com estimativa final de demanda na faixa de 10.100 a 11.300 EPS.

Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE

Item	Tipo de equipamento	Qde.
1	Sistemas Núcleo de Alto Volume	2
2	Sistemas Núcleo de Médio Volume	3
3	Infraestrutura de Segurança Típica	2
4	Soluções de Autenticação	7

5	Soluções de Serviços de Rede	39
6	Soluções IaaS/PaaS	0
7	Soluções Núcleo SaaS	1
8	Soluções Anti-Malware	1
9	Soluções de Criptografia	1
10	Registros de Servidores Web/Email	264
11	Soluções de Gerenciamento de Inventário	1
12	Soluções de HIPS e Decepção	1
13	Soluções de Borda SaaS	0
14	Registros de Servidores	42
15	Registros de Estações de Trabalho/Hosts	9050
16	Sistemas de Rede	1275

4.6.1.2. Calculadora de EPS: https://teskalabs.com/products/logman.io/eps-calculator/ com demanda de 5.873 EPS, conforme mostrado abaixo:

TeskaLabs SIEM and Log Management EPS Calculator

Sizing your Log Management and SIEM solution right is important and not an easy task. The solution is to make an analysis of your infrastructure as it directly impacts your Log Management / SIEM and the storage required to operate it efficiently. The two key numbers are Events per Second (EPS) and Gigabytes per Day (GB/day) indicating the volume of data processed in your IT infrastructure.

The calculation is based on the number of types of devices (nodes) in your IT infrastructure, which includes servers, routers, switches, firewalls and other network devices and applications.

Events Per Second (EPS) define the number of events or processes that take place in a given time on any IT appliance in your IT infrastructure.

Log Sources	Count	EPS	Daily volume
Windows desktops	9050	45.25	18.1 GB
Windows Servers	7	28	1.7 GB
Linux Servers	10	30	716.8 MB
Application Firewalls	1	30	716.8 MB
Network Firewalls	2	320	6.0 GB
Network Routers	2	2	41.0 MB

Network Switches	625	1250	12.5 GB
Network Flows	0	0	0.0 GB
Network Wireless LAN	650	3250	39.0 GB
Network Load Balancers	1	5	61.4 MB
Network IPS/IDS	1	100	2.4 GB
Network VPN	2	4	102.4 MB
Network Web Proxy	1	20	1.0 GB
Other Network Devices	0	0	0.0 GB
Hypervisor (Microsoft Hyper-V, VMware ESXi etc)	31	465	37.5 GB
WebServers	251	251	555.2 MB
Database	42	42	74.4 MB
Mail Servers	13	26	57.5 MB
Antivirus, DLP, EDR, etc.	1	5	11.1 MB
Other applications	0	0	0.0 GB
Custom		0	0 GB
	Total	5873	120.5 GB

4.6.1.3. Calculadora de EPS: https://siemsizingcalculator.logpoint.com/ com demanda de 6.226,53 EPS, conforme mostrado abaixo:

LOGPOINT Contact About Us

Infrastructure

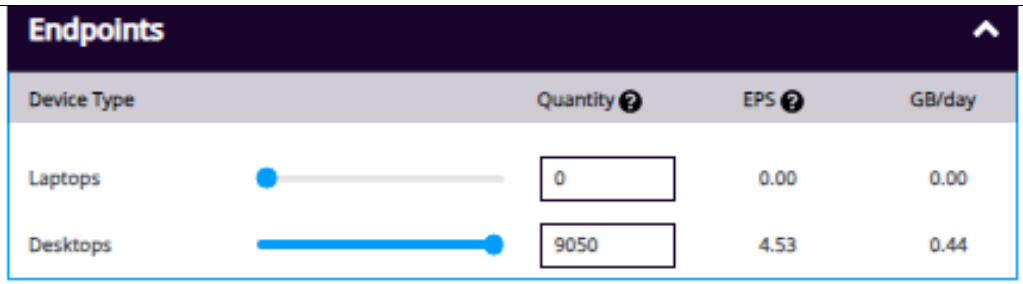
Device Type	Quantity	EPS	GB/day
Windows Servers - HIGH EPS (Event Log)	7	49.00	4.73
Windows Servers - MED EPS (Event Log)	1	3.00	0.29
Windows Servers - LOW EPS (Event Log)	0	0.00	0.00
Linux Servers	10	30.00	0.72
Unix Servers	0	0.00	0.00
Network Wireless LAN	650	3250.00	39.23
Hypervisor (ESXi, Hyper-V etc)	31	465.00	37.42
Web Servers	251	251.00	5.05
Email Servers	0	0.00	0.00

Security

Device Type	Quantity	EPS	GB/day
Network Firewalls (Layer 7 Internal)	1	240.00	9.66
Network Firewalls (Layer 7 - DMZ)	0	0.00	0.00
Network Firewalls (Internal)	2	480.00	9.66
Network Firewalls (DMZ)	2	100.00	2.01
Network IPS/IDS	1	100.00	2.41
Antivirus	0	0.00	0.00
Data Loss Protection (DLP)	0	0.00	0.00
Others	0	0.00	0.00

Network

Device Type	Quantity	EPS	GB/day
VPN Server	1	2.00	0.05
Network Routers	2	2.00	0.04
Switches	625	1250.00	10.06



Endpoints

Device Type	Quantity	EPS	GB/day
Laptops	0	0.00	0.00
Desktops	9050	4.53	0.44

4.6.1.4. Calculadora de EPS: https://positka.in/siem-sizing-calculator com demanda de 8.304 EPS, conforme mostrado abaixo:

SIEM Sizing Calculator – Calculate your infrastructure EPS

Design an efficient plan for sizing SIEM as per your infrastructure with our ha calculator. The calculation is based on the volume of data ingested to the SIE devices in your IT infrastructure.

Data Source	Number of Devices (endpoints)	In monitoring scope? (Yes / No)	Estimated EPS per day
Network and security			
User Authentication / SSO / PAM / IAM	1	Yes	10
Active Directories, Domain Controlers	7	Yes	70
Switches (syslog)	625	Yes	1250
Routers (syslog)	2	Yes	2
Wireless Access Points	650	Yes	3250
Firewalls	2	Yes	400
DDoS Protection	0	Yes	0
VPNs	1	Yes	5
Proxy Systems	1	Yes	20
Vulnerability Scanners	1	Yes	5

IDS / IPS	1	Yes	15
Threat Intelligence Feeds	0	Yes	0
Data Loss/Leakage Prevention (DLP)	0	Yes	0
EDR (Endpoint Detection & Response)	0	Yes	0
WAF (Web Application Firewall)	1	Yes	30
Network Load Balancers	1	Yes	5

Infrastructure and applications			
Windows Servers (physical and virtual)	7	Yes	105
Unix Servers (physical and virtual)	10	Yes	30
Virtual Infrastructure Servers (Hypervisor)	31	Yes	465
Web Servers	251	Yes	2510
Application Servers	13	Yes	65
Database Instances	42	Yes	42
Storage Arrays	0	Yes	0

Cloud			
Cloud Services - Azure	0	Yes	0
Cloud Services - AWS	0	Yes	0
Cloud Services - Google	0	Yes	0
SaaS	1	Yes	25
Totals	1648		8304

4.6.2. A variação de EPS de ferramentas SIEM de múltiplos fabricantes, em uma mesma infraestrutura de redes, pode ser influenciada por vários fatores, incluindo o desempenho e eficiência da ferramenta, a capacidade de processamento do hardware subjacente e a otimização das configurações da ferramenta para o ambiente específico.

Cada fabricante de SIEM pode ter implementações e abordagens diferentes para a coleta, processamento e análise de eventos de segurança. Essas diferenças podem impactar diretamente a capacidade do SIEM de lidar com um grande volume de eventos por segundo.

4.6.3. Os cálculos mostrados no item 4.6.1 são dados sobredimensionados porque na implantação podem haver ferramentas que diminuam a demanda de EPS (exemplo: EDR ou XDR) e nem todos os ativos podem ser considerados necessários para monitoramento. Sendo assim, a quantidade demandada de EPS é incerta (relatada pelos próprios fabricantes) até ser evidenciado na implantação da solução SIEM. Para não existir risco de contratar uma quantidade maior de EPS do que a mínima possível implantada, e conforme orientação de fornecedores, serão demandados inicial e aproximadamente 30% da maior estimativa de EPS levantada (item 4.6.1.1). Ou seja, a CONTRATADA deve fornecer o serviço de solução SIEM com funcionamento de 3.000 EPS por 36 meses a partir do TRD de implantação.

4.6.4. Como estratégia de complementação de EPS, a CONTRATADA deve oferecer a possibilidade de fornecer até 10 pacotes adicionais, usados sob demanda, de 500 EPS, 1.000 EPS ou 2.000 EPS cada um (ver serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação). Os pacotes adicionais podem ser demandados de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual. Portanto, os quantitativos de pacotes de EPS contratados representam meramente uma estimativa de utilização de serviço. Não haverá obrigação do TJCE na utilização do quantitativo parcial ou total dos pacotes de extra que são apresentados nos serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação. Somente serão devidos e pagos os pacotes adicionais efetivamente prestados e demandados através das respectivas Ordens de Serviço. A quantidade de pacotes adicionais demandados pode ser redimensionado em qualquer momento para quantidades maiores ou anualmente em quantidade menor (dentro da duração do contrato) e em função da mudança de monitoramento demandado pelo TJCE.

4.7. Serviço de monitoramento e correlação de eventos de segurança da informação

4.7.1. As atividades do Serviço de monitoramento e correlação de eventos de segurança da informação serão medidas por Níveis Mínimos de Serviço.

4.7.2. Os profissionais alocados no serviço de monitoramento e correlação de eventos (Analista SIEM) serão integrantes das operações no SOC conforme perfil descrito no

item 4.8.

4.7.3. A CONTRATADA deverá disponibilizar, nas instalações do TJCE (Fortaleza/CE), o acesso de leitura a console das tecnologias que suportam os serviços de Gestão de Vulnerabilidades e de Coleta, Análise e Correlação de Logs (SIEM).

4.7.4. Monitoramento 24x7x365 da infraestrutura de TI, utilizando a ferramenta SIEM como sua tecnologia base, conforme apresentado na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE e futuras expansões ou modificações.

4.7.5. A CONTRATADA deverá adotar uma abordagem preventiva e reativa, identificando eventos suspeitos, classificando os incidentes de cibersegurança e fornecendo ao TJCE um relatório para cada evento identificado.

4.7.6. A CONTRATADA terá a responsabilidade de identificar e classificar os eventos de segurança utilizando a ferramenta de SIEM. O Blue Team, com apoio do serviço de monitoramento e o Red Team, será responsável por tratar o evento no serviço/host indicado no relatório fornecido pela CONTRATADA.

4.7.7. O serviço de SIEM deverá oferecer ao TJCE as seguintes facilidades:

4.7.7.1. Monitoração de correlação de eventos.

4.7.7.2. Gestão de incidentes.

4.7.7.3. Criação de novas regras de correlação e casos de uso e detecção.

4.7.7.4. Inteligência de ameaças e conformidade.

4.7.8. Triagem de incidentes identificados pelo serviço de monitoramento.

4.7.8.1. É necessário realizar uma triagem inicial nos chamados abertos pela monitoração de segurança, identificando e agrupando os potenciais incidentes que possuam características semelhantes, como ataques direcionados ao mesmo servidor, ataques originados do mesmo IP ou múltiplas falhas de login, por exemplo.

4.7.8.2. Após a etapa de triagem inicial, os chamados devem ser avaliados para determinar se são resultantes de falsos positivos/negativos, além disso, serão realizados testes para verificar a veracidade do incidente detectado.

4.7.9. Problemas identificados pelo serviço de monitoramento.

4.7.9.1. A equipe da CONTRATADA deve abrir chamados de problema em seu próprio sistema e no sistema do TJCE, relacionados ao serviço de monitoração, a fim de identificar a causa raiz. O Blue Team, com o suporte do serviço de monitoramento e o Red Team, deve solucionar o(s) problema(s) identificado(s) ao atender as demandas de incidentes.

4.7.9.2. Os chamados devem ser atendidos pelo Blue Team, com o apoio do serviço de monitoramento.

4.7.10. Incidentes de segurança identificados pelo serviço de monitoramento.

4.7.10.1. O Blue Team, com o suporte do serviço de monitoramento e o Red Team, será responsável por lidar com todo tipo de incidente e executar os procedimentos de resposta (item 2.3.13) para que seja implementada a respectiva solução.

4.7.10.2. O TJCE deve ser notificado sobre os incidentes por meio do sistema de chamados, e-mail e/ou telefone, conforme acordado previamente com o TJCE, de acordo com as necessidades de comunicação interna e/ou externa.

4.7.10.3. A CONTRATADA deve fornecer informações sobre os incidentes ao TJCE, por meio da abertura de chamados na ferramenta de ITSM do TJCE.

4.7.11. Ocorrência de Incidentes no serviço de monitoramento.

4.7.11.1. Em caso de detecção de algum incidente de segurança, a CONTRATADA deve contatar imediatamente o TJCE por telefone, e-mail e abertura de chamado na ferramenta de ITSM do TJCE. Isso é necessário para que sejam tomadas as medidas corretivas e legais adequadas, tanto pela equipe da CONTRATADA quanto, se necessário, com a colaboração da equipe do TJCE, seguindo o procedimento estabelecido para resposta a incidentes (item 2.3.13).

4.7.11.2. O serviço de monitoramento deve comunicar imediatamente ao TJCE sobre acessos indevidos, instalação de códigos maliciosos ou qualquer outra ação que represente um risco para a segurança do ambiente do TJCE. Isso deve ser feito mesmo se essas tentativas não forem bem-sucedidas, mas houver persistência por parte do agente mal-intencionado.

4.7.11.3. O serviço de monitoramento deve fornecer todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que os incidentes de segurança relatados possam ser investigados pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12. Resposta a incidentes no serviço de monitoramento.

4.7.12.1. A CONTRATADA deve incluir as informações necessárias, como origem do ataque, tipo de ataque, data e hora, logs, causa do incidente de segurança e o procedimento de resposta ao incidente na ferramenta de ITSM do TJCE, a fim de possibilitar a implementação das medidas corretivas necessárias

pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12.2. Os incidentes de segurança devem estar relacionados a eventos de segurança das soluções monitoradas e podem incluir, mas não se limitar a, acessos indevidos, instalações de códigos maliciosos, indisponibilidade de serviços devido a ataques de negação de serviço (DoS e DDoS), ataques por força bruta ou qualquer outra ação que possa comprometer a confidencialidade, disponibilidade ou integridade das informações do TJCE.

4.7.13. Software e Hardware necessários para a solução SIEM no serviço de monitoramento.

4.7.13.1. A CONTRATADA é responsável por fornecer os softwares e hardwares necessários para implantar os serviços gerenciados de monitoramento e correlação de eventos de segurança da informação, durante o prazo do contrato e sem custos adicionais para o TJCE.

4.7.14. Configuração do *Security Information and Event Management* (SIEM).

4.7.14.1. A CONTRATADA deverá ativar o serviço que será utilizado como ferramenta, durante a vigência do contrato e antes do TRD de implantação, para prestação do Serviço de Coleta, Análise e Correlação de Logs, através de uma solução SIEM.

4.7.14.2. A CONTRATADA deve realizar a implementação das configurações, regras e políticas apropriadas para o ambiente do TJCE, levando em consideração as necessidades específicas do ambiente.

4.7.14.3. O TJCE, com o suporte da CONTRATADA, será responsável por realizar as configurações nos equipamentos de rede (switches, roteadores, servidores, etc.), servidores Linux/Windows e equipamentos de segurança da informação do TJCE para enviar os logs para a solução de SIEM. Adicionalmente, as configurações na solução de SIEM são de responsabilidade da CONTRATADA.

4.7.14.4. As configurações, regras de correlação, alertas e outras configurações do SIEM serão implementadas pela CONTRATADA e de propriedade intelectual e responsabilidade exclusiva do TJCE. Portanto, essas configurações não devem ser extraídas, copiadas, manipuladas ou removidas sem o consentimento expresso do TJCE.

4.7.14.5. A Solução de SIEM deve abrir automaticamente chamados na ferramenta de ITSM do TJCE sempre que detectar um possível incidente de

disponibilidade ou segurança.

4.7.14.6. Toda a mão de obra especializada necessária para a instalação e configuração da solução de SIEM deve ser fornecida pela CONTRATADA.

4.7.14.7. A CONTRATADA é responsável por executar todas as operações de monitoramento, gerenciamento e administração da solução de SIEM, conforme determinação do TJCE, abrangendo, mas não se limitando a:

1. Coleta de logs.
2. Criação de regras de correlação, não havendo limite mínimo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados.
3. Realização de configurações do SIEM (agentes, regras de incidentes, regras de correlação, etc).
4. Interação com o fabricante da solução.
5. Backup e restore.
6. Resolução de problemas.
7. Suporte.
8. Instalação de serviços relativos ao escopo contratado.
9. Atualização, de acordo com as recomendações do fabricante.
10. Outras operações citadas nos itens 4.3, 4.4 e 4.5.

4.7.14.8. Durante a fase de implantação, a CONTRATADA deve apresentar um conjunto de regras pré-definidas para ativação. Essas regras só serão implementadas após a aprovação do TJCE.

4.7.14.9. CONTRATADA será responsável por documentar as regras aprovadas pelo TJCE. A documentação de regras aprovadas (novas ou atualizadas) deve seguir os processos de gerenciamento de mudanças do TJCE.

4.7.14.10. O TJCE tem permissão para solicitar alterações nas regras de correlação de eventos, de forma a ajustá-las às suas necessidades.

4.7.14.11. A CONTRATADA deverá prestar todos os serviços relativos ao SIEM (implantação, configuração, manutenção, análise de logs, detecção/resposta a incidentes, backup e restore, etc), conforme requisitos de funcionamento do SIEM apresentados nos itens 4.1 até 4.6.

4.7.14.12. A operação da console de administração e operação deverá ser de responsabilidade exclusiva da CONTRATADA, conforme especificações técnicas dos itens 4.1 até 4.6.

4.7.14.13. É de responsabilidade da CONTRATADA realizar a integração do SIEM de

forma a possibilitar o recebimento de alertas e a abertura automática de incidentes na ferramenta de ITSM do TJCE.

4.8. Perfil dos profissionais do Analista de Segurança Sênior - SIEM.

4.8.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS, contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 12 meses.

4.8.2. Deve contar com a certificação relacionada e emitida pelo fabricante da ferramenta SIEM usada no serviço de monitoramento e correlação de eventos.

4.8.3. Deve contar com proficiência de inglês intermediário para poder estabelecer comunicação com a comunidade técnica do fabricante da ferramenta SIEM, com o objetivo de obter informações que ajudem na implantação, execução, configuração e manutenção da ferramenta SIEM.

4.8.4. Deve contar com especialização em segurança da informação, comprovada através de certificado de conclusão oudiploma emitido por instituição de ensino superior reconhecida pelo Ministério da Educação ou com, pelo menos, uma das seguintes certificações: CompTIA Security+; EXIN Information Security Foundation; EXIN Ethical Hacking Foundation; GIAC Security Essentials (GSEC).

5. NÍVEIS MÍNIMOS DE SERVIÇO

5.1. Os Níveis Mínimos de Serviço (NMS) são parâmetros claros e mensuráveis que têm como objetivo avaliar e verificar vários aspectos dos serviços contratados, incluindo qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança. Esses critérios são estabelecidos de forma objetiva para garantir a excelência na prestação dos serviços.

5.2. Os serviços serão avaliados por meio de indicadores e NMS estabelecidos em fórmulas de cálculo específicas.

5.3. A responsabilidade de cumprir os NMSs é da CONTRATADA. A avaliação será realizada pela equipe de fiscalização do TJCE mensalmente, levando em consideração as metas exigidas dos serviços, conforme descrito na Tabela 4. Indicadores de Nível de Serviço. Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento (pontos) serão cumulativas.

5.4. A empresa contratada é responsável por manter os padrões de qualidade estabelecidos para a prestação dos serviços, conforme Tabela 4. Indicadores de Nível de Serviço e Tabela 5. Glosas por descrição de referências para todos os serviços contratados.

5.5. A CONTRATADA terá uma redução de 2% (dois por cento) sobre o valor da fatura referente ao mês de ocorrência, a cada 15 pontos, ou um valor proporcional de redução de 2% a cada 15 pontos de glosa. Exemplo: para uma glosa de 10 pontos, a redução será de 1,33% como resultado da conta proporcional (10/15)*2%.

5.6. A meta exigida estabelece o valor exato (=), o limite máximo (<=) ou o limite mínimo (>=) que a CONTRATADA deve alcançar para cada um dos indicadores.

5.7. A meta exigida do cálculo com base no mês calendário será aplicado ao menor valor instantâneo entre os indicadores relativos aos horários de expediente regular ou horários de plantão contínuo. Por exemplo, um incidente que tenha sido inicializado no horário de plantão contínuo faltando 5 minutos para que comece o horário de expediente regular, passará a ter a menor meta entre ambos horários (após os 5 minutos) até a sua solução. Da mesma forma, um incidente que tenha sido inicializado no horário de expediente regular faltando 5 minutos para que comece o horário de plantão contínuo, passará a ter a menor meta (após os 5 minutos) entre ambos horários até a sua solução.

5.8. A CONTRATADA será responsável apenas pelos índices relacionados às solicitações de serviços e incidentes atribuídos a ela. Ela não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outras equipes do TJCE, nem por situações dependentes de terceiros, que, portanto, não serão consideradas para fins de cálculo.

5.9. Requisições de serviço e incidentes reabertos referem-se a solicitações de serviço ou incidentes que foram considerados resolvidos, mas ainda estão pendentes de solução.

Tabela 4. Indicadores de Nível de Serviço

Serviço da Tabela 1	Nº	Indicadores de Nível de Serviço	Cálculo com base no mês calendário	Meta Exigida	Glosa
1, 2 e 3	1	Atividades rotineiras mensais definidas nos itens 2, 3 e 4, e programadas de acordo com o Plano de Trabalho ou por Requisição de Serviço.	Tempo = (Horas investidas nas atividades programadas) – ([Horas acordadas na OS]*1,25)	<=0 minutos	60 pontos
1 e 3	2	Índice de disponibilidade dos serviços de monitoramento e correlação de eventos (SIEM).	100 * [(Total de tempo com disponibilidade no mês – com exceção de indisponibilidade de energia ou link de conexão) / (Total de tempo no mês)] %	>= 99,7%	5 pontos (+2 pontos a cada hora excedente)
	3	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de expediente regular.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
	4	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 180 minutos	30 pontos (+5 pontos a cada 20 minutos excedentes)
	5	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de expediente regular.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 120 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	6	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 240 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	7	Tempo máximo de não acompanhamento a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de expediente regular.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 15 minutos	10 pontos (+5 pontos a cada 10 minutos excedentes)
	8	Tempo máximo de não acompanhamento a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de plantão contínuo.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 45 minutos	10 pontos (+5 pontos a cada 10 minutos excedentes)
	9	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados por outras equipes e em horário de expediente regular.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
	10	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 90 minutos	5 pontos (+2 pontos a cada 10 minutos

		por outras equipes e em horário de plantão contínuo.			excedentes)
	11	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente.	Tempo = (Hora de conclusão do planejamento da requisição de mudança) – (Hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente)	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)
	12	Tempo máximo para abertura de chamados de suporte com terceiros. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de abertura do chamado) – (Hora da triagem)	<= 30 minutos	5 pontos (+2 pontos a cada 5 minutos excedente)
1	13	Tempo máximo para resolução de requisições de serviços relacionados aos Produtos de UTM, NGFW, EDR, WAF, Gestor de vulnerabilidades. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 180 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
	14	Tempo máximo para resolução de requisições de serviços relacionados a outros ativos de segurança da informação.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 30 horas	10 pontos (+3 pontos a cada hora excedente)
	15	Tempo máximo para triagem de incidentes de segurança e em horário de expediente regular.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 15 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	16	Tempo máximo para triagem de incidentes de segurança e em horário de plantão contínuo.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 120 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	17	Tempo máximo para resposta de incidentes de segurança de gravidade alta e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 60 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	18	Tempo máximo para resposta de incidentes de segurança de gravidade alta e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 480 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	19	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 150 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	20	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	21	Tempo máximo para resposta de incidentes de segurança de gravidade baixa e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 210 minutos	5 pontos (+2 pontos a cada hora excedente)
	22	Tempo máximo para resposta de incidentes de segurança de gravidade	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	5 pontos (+2 pontos a cada

		baixa e em horário de plantão contínuo.			hora excedente)
	23	Tempo máximo para comunicação de incidentes a central de serviços da CONTRATADA e à equipe de segurança do TJCE. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora da comunicação) – (Hora da triagem)	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes)
2	24	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço.	Tempo = (Horas investidas na Requisição de Serviço) – ([Horas acordadas na OS]*1,25)	<=0 minutos	15 pontos

Tabela 5. Glosas por descrição de referências para todos os serviços contratados

Nº	Descrição	Referência	Glosa
1	Não implementar a coleta de logs (via coletores), sua integração com a ferramenta SIEM e a retenção de logs após o período de carência de glossa.	Por ocorrência e por dia	15 pontos
2	Deixar de disponibilizar presencialmente no TJCE o Red Team, conforme descrito no item 1.3.1.	Por ocorrência e por dia	15 pontos
3	Deixar de fornecer os documentos comprobatórios de qualificação de qualquer profissional.	Por ocorrência e por dia	15 pontos
4	Deixar de documentar atividades rotineiras ou de requisição de serviço na ferramenta de ITSM.	Por ocorrência	5 pontos
5	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, mesmo em situações de substituição temporária.	Por profissional e por dia	15 pontos
6	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	50 pontos
7	Suspender, colocar como pendente, pausar ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	5 pontos
8	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável.	Por regra incluída, alterada ou excluída	10 pontos
9	Fraudar, manipular ou descaracterizar indicadores, metas de níveis de serviço e de desempenho por quaisquer subterfúgios.	Por ocorrência	100 pontos
10	Deixar de cumprir qualquer outra obrigação estabelecida no contrato e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10 pontos
11	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	180 pontos
12	Causar qualquer dano aos equipamentos do TJCE por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50 pontos
13	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10 pontos
14	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo TJCE.	Por ocorrência	10 pontos
15	Incluir, excluir ou alterar regras nos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	20 pontos
16	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada ou Rotineira.	Por ocorrência	10 pontos
17	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique, sem prejuízo de outras sanções legais e das cabíveis penais previstas no art. 156, da Lei n. 14.133/2021.	Por ocorrência	60 pontos
18	Deixar de apresentar relatórios, levantamentos ou inventários no prazo determinado em comum acordo.	Por ocorrência	15 pontos

19	Deixar de comunicar o contratante da substituição de profissionais responsáveis pela execução das atividades.	Por ocorrência	30 pontos
20	Deixar de atuar tempestivamente no caso de incidentes graves.	Por ocorrência	60 pontos
21	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
22	Deixar de cumprir ou implementar as rotinas em conformidade com os processos de trabalho do TJCE e da Diretoria de Tecnologia da Informação	Por ocorrência	10 pontos
23	Deixar de apresentar mensalmente propostas de melhorias no ambiente	Por ocorrência	5 pontos
24	Deixar de notificar sobre ocorrências recorrentes.	Por ocorrência	5 pontos

ANEXO II DO CONTRATO

PJSETIN2015001 – Fábrica de Software

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no _____ sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no CONTRATANTE.

CIÊNCIA
CONTRATADA – Funcionários

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____,_____ de _____ de 20_____.

ANEXO III DO CONTRATO
TERMO DE COMPROMISSO

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado em Av. General Afonso Albuquerque Lima, S/N. – Cambeba, Fortaleza-CE CEP:60822-325 – Fone: (85) 3207-7000, CNPJ n° 09.444.530/0001-01, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____, nº _____, _____, _____/__, CEP: __.___-___, CNPJ n° ___.___.___/____-__, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º __/20__ doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente

ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº. 14.133/21.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro de Fortaleza-CE, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ Matrícula:	ASSINADO DIGITALMENTE YURE LEOPOLDO SABINO DE FREITAS A conformidade com a assinatura pode ser verificada em: http://serpro.gov.br/assinador-digital SERPRO _____ Representante Legal
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ Preposto da Contratada	_____ Fiscal Técnico

_____, _____ de _____ de 20____

ANEXO IV DO CONTRATO
PROPOSTA DA CONTRATADA

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
COMISSÃO DE LICITAÇÃO
Ref. PREGÃO N. 019/2023.
PROCESSO N. 8521639-33.2023.8.06.0000

APRESENTAÇÃO DA PROPOSTA, CONFORME MODELO DO ANEXO 3 DO EDITAL

Empresa: NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ: 05.250.796/0001-54
Endereço/Telefone: Av. Pontes Vieira, 2340 - Dionísio Torres, UNO - Medical & Office - Sala 510 - 514 - 5º andar, CEP: 60135-238 – Fortaleza/CE Telefone: (85) 3195-2200 / 2231 / 2212
Insc. Estadual/Municipal: 06.180540-8 / 176407-1
Endereço Eletrônico (e-mail): licitacoes@networksecure.com.br

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Serviço de gestão de incidentes de segurança (Blue Team)	Mês	36	R$ 43.911,00	R$ 1.580.796,00
2	Serviço de gestão testes de invasão (Red Team)	Mês	36	R$ 24.700,00	R$ 889.200,00
3	Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS	Mês	36	R$ 47.158,19	R$ 1.697.694,84
4	Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses	Pacote	10	R$ 11.879,00	R$ 118.793,00
5	Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses	Pacote	10	R$ 23.051,00	R$ 230.516,00
6	Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses	Pacote	10	R$ 42.300,00	R$ 423.000,00
VALOR GLOBAL					**R$ 4.939.999,84**

VALOR GLOBAL:.R$ 4.939.999,84 (Quatro milhões, novecentos e trinta e nove mil, novecentos e noventa e nove reais e oitenta e quatro centavos).

O prazo de validade da proposta é de 90 (noventa) dias, contados a partir da data da sua apresentação, razão pela qual a não manutenção das propostas no decorrer de seu prazo de validade poderá ensejar as sanções previstas no art. 90, §5º da Lei n. 14.133/2021;

Declaramos que nos valores propostos estão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos produtos..

DADOS DO REPRESENTANTE LEGAL, RESPONSÁVEL PELA ASSINATURA DO CONTRATO:

Nome: Yure Leopoldo Sabino De Freitas
Cargo: Diretor Comercial
Endereço: Rua General Tertuliano Potiguara, 158, Apto 701, Aldeota, CEP: 60135-280 - Fortaleza/CE
Cart. Ident. nº.: 559056187 **Expedido por:** SPP-SP
CPF: 525.285.023-20

Fortaleza/CE, 26 de Janeiro de 2024

YURE LEOPOLDO SABINO DE FREITAS

Assinado de forma digital por YURE LEOPOLDO SABINO DE FREITAS
Dados: 2024.01.26 17:17:16 -03'00'

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ Nº 05.250.796/0001-54
Yure Leopoldo Sabino De Freitas
Diretor Comercial
CPF Nº 525.285.023-20

ANEXO V DO TERMO DE CONTRATO

POLÍTICA DO BANCO INTERAMERICANO DE DESENVOLVIMENTO SOBRE PRÁTICAS PROIBIDAS

1.1 O Banco requer que todos os Mutuários (incluindo beneficiários de doações), Agências Executoras ou Agências Contratantes, bem como todas as empresas, entidades ou pessoas físicas que estejam apresentando propostas ou participando de atividades financiadas pelo Banco, incluindo, *inter alia*, solicitantes, concorrentes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e agentes, quer com atribuições expressas ou implícitas), observem os mais altos padrões éticos, e denunciem ao Banco[1] todos os atos suspeitos de constituir uma Prática Proibida da qual tenha conhecimento ou seja informado, durante o processo de seleção e negociação ou na execução de um contrato. As Práticas Proibidas compreendem atos de: (a) práticas corruptas; (b) práticas fraudulentas; (c) práticas coercitivas; (d) práticas colusivas e (e) práticas obstrutivas. O Banco estabeleceu mecanismos para denúncia de suspeitas de Práticas Proibidas. Qualquer denúncia deverá ser apresentada ao Escritório de Integridade Institucional (EII) do Banco para que se realize a devida investigação. O Banco também estabeleceu procedimentos de sanção para a resolução de casos. Além disso, o Banco celebrou acordos com outras instituições financeiras internacionais (IFI) visando ao reconhecimento recíproco às sanções aplicadas pelos respectivos órgãos de sanção.

(a) Para fins de cumprimento dessa política, o Banco define os termos indicados a seguir:

(i) uma *prática corrupta* consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar as ações de outra parte;

(ii) uma *prática fraudulenta* é qualquer ato ou omissão, incluindo uma declaração falsa que engane ou tente enganar uma parte para obter benefício financeiro ou de outra natureza ou para evitar uma obrigação;

(iii) uma *prática coercitiva* consiste em prejudicar ou causar dano ou na ameaça de prejudicar ou de causar dano, direta ou indiretamente, a qualquer parte ou propriedade da parte para influenciar indevidamente as ações de uma parte;

(iv) uma prática colusiva é um acordo entre duas ou mais partes efetuado com o intuito de alcançar um propósito impróprio, incluindo influenciar impropriamente as ações de outra parte; e

(v) uma prática obstrutiva consiste em:

(aa) destruir, falsificar, alterar ou ocultar deliberadamente uma evidência significativa para a investigação ou prestar declarações falsas aos investigadores com o fim de obstruir materialmente uma investigação do Grupo do Banco sobre denuncias de uma prática corrupta, fraudulenta, coercitiva ou colusiva; e/ou ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes

para a investigação ou a continuação da investigação,

(bb) ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação do Grupo BID ou a continuação da investigação; ou

(cc) todo ato que vise a impedir materialmente o exercício de inspeção do Grupo BID e dos direitos de auditoria previstos no parágrafo 1.1(f) a seguir; e

(vi) A "apropriação indevida" consiste no uso de fundos ou recursos do Grupo BID para um propósito indevido ou para um propósito não autorizado, cometido de forma intencional ou por negligência grave.

(b) Se, em conformidade com os procedimentos de sanções do Banco, for determinado que em qualquer estágio da aquisição ou da execução de um contrato qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e agentes, quer sejam suas atribuições expressas ou implícitas), estiver envolvida em uma Prática Proibida em qualquer etapa da adjudicação ou execução de um contrato, o Banco poderá:

(i) não financiar nenhuma proposta de adjudicação de um contrato para obras, bens e serviços relacionados financiados pelo Banco;

(ii) suspender os desembolsos da operação se for determinado, em qualquer etapa, que um empregado, agente ou representante do Mutuário, do Órgão Executor ou da Agência Contratante estiver envolvido em uma Prática Proibida;

(iii) declarar uma aquisição viciada e cancelar e/ou declarar vencido antecipadamente o pagamento de parte de um empréstimo ou doação relacionada inequivocamente com um contrato, se houver evidências de que o representante do Mutuário ou Beneficiário de uma doação não tomou as medidas corretivas adequadas (incluindo, entre outras medidas, a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um período que o Banco considere razoável;

(iv) emitir advertência à empresa, entidade ou pessoa física com uma carta formal censurando sua conduta;

(v) declarar que uma empresa, entidade ou pessoa física é inelegível, permanentemente ou por um período determinado, para: (i) adjudicação de contratos ou participação em atividades financiadas pelo Banco; e (ii) designação[2] como subconsultor, subempreiteiro ou fornecedor de bens ou serviços por outra empresa elegível a qual tenha sido adjudicado um contrato para executar atividades financiadas pelo Banco;

(vi) encaminhar o assunto às autoridades competentes encarregadas de fazer cumprir a lei; e/ou;

(vii) impor outras sanções que julgar apropriadas às circunstâncias do caso, inclusive multas que representem para o Banco um reembolso dos custos referentes às investigações e ao processo. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções acima referidas.

(c) O disposto nos parágrafos 1.1 (b) (i) e (ii) se aplicará também nos casos em que as partes tenham sido temporariamente declaradas inelegíveis para a adjudicação de novos contratos, na pendência da adoção de uma

decisão definitiva em um processo de sanção ou qualquer outra resolução.

(d) A imposição de qualquer medida que seja tomada pelo Banco conforme as disposições anteriormente referidas será de caráter público.

(e) Além disso, qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), poderá ser sujeita a sanções, em conformidade com o disposto nos acordos que o Banco tenha celebrado com outra instituição financeira internacional com respeito ao reconhecimento recíproco de decisões de inelegibilidade. Para fins do disposto neste parágrafo, o termo "sanção" refere-se a toda inelegibilidade permanente, imposição de condições para a participação em futuros contratos ou adoção pública de medidas em resposta a uma contravenção às regras vigentes de uma IFI aplicável à resolução de denúncias de Práticas Proibidas;

(f) O Banco exige que os solicitantes, concorrentes, fornecedores e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, prestadores de serviços e concessionárias permitam que o Banco revise quaisquer contas, registros e outros documentos relativos à apresentação de propostas e a execução do contrato e os submeta a uma auditoria por auditores designados pelo Banco. Solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias deverão prestar plena assistência ao Banco em sua investigação. O Banco requer ainda que todos os solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias: (i) mantenham todos os documentos e registros referentes às atividades financiadas pelo Banco por um período de sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; e (ii) forneçam qualquer documento necessário à investigação de denúncias de Práticas Proibidas e assegurem-se de que os empregados ou representantes dos solicitantes, concorrentes, fornecedores de bens e seus representantes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às consultas relacionadas com a investigação provenientes de pessoal do Banco ou de qualquer investigador, agente, auditor ou consultor devidamente designado. Caso o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária se negue a cooperar ou descumpra o exigido pelo Banco, ou de qualquer outra forma crie obstáculos à investigação por parte do Banco, o Banco, a seu critério, poderá tomar medidas apropriadas contra o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária.

(g) Se um Mutuário fizer aquisições de bens, obras, serviços que forem ou não de consultoria diretamente de uma agência especializada, todas as disposições da Seção 8 relativas às sanções e Práticas Proibidas serão aplicadas integralmente aos solicitantes, concorrentes, fornecedores e seus representantes, empreiteiros, consultores,

pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), ou qualquer outra entidade que tenha firmado contratos com essa agência especializada para fornecer tais bens, obras, serviços que forem ou não de consultoria, em conformidade com as atividades financiadas pelo Banco. O Banco se reserva o direito de obrigar o Mutuário a lançar mão de recursos tais como a suspensão ou a rescisão. As agências especializadas deverão consultar a lista de empresas ou pessoas físicas declaradas temporária ou permanentemente inelegíveis pelo Banco. Caso alguma agência especializada celebre um contrato ou uma ordem de compra com uma empresa ou uma pessoa física declarada temporária ou permanentemente inelegível pelo Banco, o Banco não financiará os gastos correlatos e poderá tomar as demais medidas que considere convenientes.

1.2 Os Concorrentes ao apresentar uma proposta declaram e garantem que:

(i) leram e entenderam a proibição sobre atos de fraude e corrupção disposta pelo Banco e se obrigam a observar as normas pertinentes;

(ii) não incorreram em nenhuma Prática Proibida descrita neste documento;

(iii) não adulteraram nem ocultaram nenhum fato substancial durante os processos de seleção, negociação e execução do contrato;

(iv) nem eles nem os seus agentes, pessoal, subempreiteiros, subconsultores ou quaisquer de seus diretores, funcionários ou acionistas principais foram declarados inelegíveis pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco, nem foram declarados culpados de delitos vinculados a práticas proibidas;

(v) nenhum de seus diretores, funcionários ou acionistas principais tenha sido diretor, funcionário ou acionista principal de qualquer outra empresa ou entidade que tenha sido declarada inelegível pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco ou tenha sido declarado culpado de um delito envolvendo Práticas Proibidas;

(vi) declararam todas as comissões, honorários de representantes ou pagamentos para participar de atividades financiadas pelo Banco; e

(vii) reconhecem que o descumprimento de qualquer destas garantias constitui fundamento para a imposição pelo Banco de uma ou mais medidas descritas na Cláusula 1.1 (b).

ANEXO VI DO CONTRATO
PAÍSES ELEGÍVEIS

Elegibilidade para Provisão de Bens, Obras e Serviços

em Contratos Financiados pelo Banco

Nota: *O termo "Banco" usado neste documentos inclui o BID, o Fumin e outros fundos administrados por ele. Dependendo da fonte de financiamento, o usuário deve selecionar uma das seguintes opções do item 1. O financiamento pode vir do BID ou do Fundo Multilateral de Investimentos (Fumin); ocasionalmente, os contratos podem ser financiados por fundos especiais que restringem ainda mais os critérios de elegibilidade a um grupo de países membros. Quando a última opção for escolhida, os critérios de elegibilidade devem ser indicados aqui*:

.....

1) Países Membros quando o financiamento provém do Banco Interamericano de Desenvolvimento.

a) Países Mutuários:

(i) Argentina, Bahamas, Barbados, Belize, Bolívia, Brasil, Chile, Colômbia, Costa Rica, Equador, El Salvador, Guatemala, Guiana, Haiti, Honduras, Jamaica, México, Nicarágua, Panamá, Paraguai, Peru, República Dominicana, Suriname, Trinidad e Tobago, Uruguai e Venezuela.

b) Países não Mutuários:

(i) Alemanha, Áustria, Bélgica, Canadá, República Popular da China, República da Coréia, Croácia, Dinamarca, Eslovênia, Espanha, Estados Unidos, Finlândia, França, Israel, Itália, Japão, Noruega, Países Baixos, Portugal, Reino Unido, Suécia e Suíça.

c) Territórios elegíveis:

(i) *Guadalupe, Guiana Francesa, Martinica, Reunião – como Estado da França*

(ii) *Ilhas Virgens dos EUA, Porto Rico, Guam – como Território dos EUA*

(iii) *Aruba – como um país integrante do Reino dos Países Baixos, assim como, Bonaire, Curaçao, Santa Marta, Saba, Santo Eustáquio – como Estados do Reino dos Países Baixos*

(IV) *Hong Kong – Região Administrativa Especial da República Popular da China.*

---

1) Critérios para determinar a nacionalidade e origem dos bens e serviços

Estas disposições de políticas tornam necessário estabelecer critérios para determinar: a) a nacionalidade das firmas e indivíduos elegíveis para participar em contratos financiados pelo Banco; e b) o país de origem dos bens e serviços. Nessas determinações, serão utilizados os seguintes critérios:

A) Nacionalidade

a) **Um indivíduo é considerado nacional** de um país membro do Banco se satisfaz um dos seguintes requisitos:

(i) é cidadão de um país membro; ou

(ii) estabeleceu seu domicílio em um país membro como residente de boa fé e está legalmente autorizado para trabalhar nesse país.

b) **Uma firma é considerada nacional** de um país membro se satisfaz os dois seguintes requisitos:

(i) está legalmente constituída ou estabelecida conforme as leis de um país membro do Banco; e

(ii) mais de cinquenta por cento (50%) do capital da firma é de propriedade de indivíduos ou firmas de países membros do Banco.

Todos os membros de um consórcio e todos os subempreiteiros devem cumprir os requisitos acima estabelecidos.

B) Origem dos Bens

Os bens tem origem em um país membro do Banco se foram extraídos, desenvolvidos, cultivados, colhidos ou produzidos em um país membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características, funções ou utilidades básicas são substancialmente diferentes de suas partes ou componentes.

No caso de um bem que consiste de vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para financiamento se a montagem dos componentes for feita em um país membro, independente da origem dos componentes. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

Para fins de determinação da origem dos bens identificados como "feito na União Européia", estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Européia.

A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina a origem dos mesmos.

C) Origem dos Serviços

O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços conforme os critérios de nacionalidade acima estabelecidos. Este critério é aplicado aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem, etc.), aos serviços de construção e aos serviços de consultoria.

ANEXO VII DO CONTRATO

FICHA DE DADOS DO REPRESENTANTE LEGAL

Dados pessoais do(s) representante(s) e/ou procurador(es), devidamente habilitados, da futura CONTRATADA, indicado(s) para assinatura do Termo de Contrato:

NOME	:	Yure Leopoldo Sabino De Freitas
ESTADO CIVIL	:	
PROFISSÃO	:	Diretor Comercial
RG	:	559056187-SPP-SP
CPF	:	525.285.023-20
DOMICÍLIO	:	Av. Pontes Vieira, nº 2340, Dionísio Torres
CIDADE	:	Fortaleza
UF	:	CE
FONE	:	(85) 3195-2200 / 2231 / 2212
CELULAR	:	
E-MAIL	:	licitacoes@networksecure.com.br