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

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

9.5. A sanção de multa calculada na forma do edital ou do 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.

9.5.1. A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o complementem, às sanções e penalidades administrativas, inclusive multas.

9.5.1.1. Caso a Contratada se torne inadimplente na execução dos serviços, a 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 no Termo de Referência, sem prejuízo das sanções legais e responsabilidades civil e criminal.

9.5.2. A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

9.5.3. Os percentuais de multas aplicadas incidirão sempre sobre do valor global do termo de contrato licitado ou celebrado ou instrumento equivalente.

9.6. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.7. Na aplicação da sanção será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.8. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no item 9.1 (incisos I, II e III), quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.9. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas no item 9.1 (incisos IV, V, VI e VII), bem como pelas infrações administrativas previstas no item 9.1 (incisos I, II e III) que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

O original deste documento é eletrônico e foi assinado digitalmente por: SERGIO MENDONÇA ALVES, MARIA NARCISO CARVALHO DE ANDRADE, CRISTIANO BATISTA PACHECO SILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento, acesse o site: https://portaldeadmin.tjpe.jus.br/atendimento/verificacao-de-documentos e informe o processo 8521639-33.2023.8.06.0000 e o código A90613LT.

9.10. A apuração de responsabilidade relacionadas 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.

9.11. 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.

9.12. 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.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

9.15. Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

9.16. 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.

9.17. 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.

9.18. Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 156 da Lei n. 14.133/21:

9.18.1. Aplicação de multa administrativa, além das Glosas previstas no item 5.7.

9.18.1.1.Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas

O original deste documento é eletrônico e foi assinado digitalmente por: juiz de direito SERGIO MENDES DE ALMEIDA, LUIZA DENISE MARIA NORONES CAGEN DA CRUZ, MELANIO BATISTA PACOSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento, acesse o site: https://portaldeassinaturas.tjce.jus.br/validar-documento e o código A906I3LT.

hipóteses de inexecução total ou violação do sigilo.

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

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

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Proposta de Preço

10.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:

10.1.1.1. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

10.1.1.2. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

10.1.1.3. Deve fazer menção ao número do pregão e do processo licitatório;

10.1.1.4. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

10.1.1.5. Deve conter na última folha o número do CNPJ da empresa;

10.1.1.6. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

10.1.1.7. Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a licitante julgar necessário;

10.1.1.8. Indicação do nome do banco, número da agência, número da conta corrente, para fins de recebimento dos pagamentos.

10.1.1.9. Objetivando facilitar e agilizar o processo de validação das especificações técnicas da Solução e como forma de comprovação, a licitante deverá anexar todas as documentações técnicas comprobatórias das características e especificações para cada item do Serviços a serem adquiridos.

10.1.1.10. Deverá ser anexado junto a sua proposta, documento contendo o item do Edital e sua referência comprobatória, informando/indicando/referenciando as referidas documentações técnicas comprobatórias.

10.2. Modalidade e Tipo de Licitação

10.2.1. A modalidade da licitação sugerida é o Pregão Eletrônico, em conformidade com a Lei

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALCANTARA NETO, SERGIO MENDONCA DE ALMEIDA, LILIAN DE DENISE MARIA NARCISO GALVAO, CRISTIANO BATISTA PACHECO SILVA. Data da última assinatura: 14/11/2023 às 08:50:17.
Para autenticar a autenticidade deste documento, acesse o site: http://portaladoma.ajpe.jus.br/atendimento/informe-o-nome-do-processo. 8521639-33.2023.8.06.0000 e o código A90613LT.

14.133/21, tendo em vista o objeto se tratar de bem e serviço comum, cujos padrões de qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

10.2.2. A licitação será do tipo menor preço. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item 7.

10.2.3. O objeto desta contratação será realizado por execução indireta, sob o regime de empreitada por Preço Unitário, nos termos dos art. 46°, I, da Lei n. 14.133/21.

10.3. Justificativa de Adoção da Modalidade da Licitação

10.3.1. Modalidade de Licitação

10.3.1.1. A contratação da solução ora pretendida é oferecida por diversos fornecedores no mercado de TIC, vez que apresenta características padronizadas e usuais. Assim, trata-se de serviço comum pois é fácil encontrar empresas no mercado que ofereçam serviços de tecnologia da informação, manutenção, suporte e garantia da Solução pretendida. Devido à alta demanda por esses serviços, no setor privado e público, há uma ampla oferta de fornecedores com diferentes níveis de expertise e qualidade e, portanto, licitação via Pregão, em sua forma eletrônica, pelo tipo menor preço individual, previamente ao menor preço individual de cada item, e modo de disputa aberto e fechado.

10.3.1.2. Nos critérios de habilitação técnica, não serão solicitados prazos de validades dos atestados de capacidade técnica, abrangendo maior competitividade no certame, sem deferir os ditames legais, vez que o objeto que será licitado é usual de mercado e não possui uma existência muito longeva, para limitar períodos. Serão solicitados documentos/atestados emitidos por fabricantes de alguns componentes, em detrimento dos vários itens tecnológicos e do alto montante orçamentário.

10.4. Qualificação Econômico-Financeira

10.4.1. A Qualificação Econômico-Financeira tem como objetivo avaliar a capacidade financeira e econômica das empresas interessadas em participar da concorrência, garantindo assim a segurança do contrato e a viabilidade do projeto. No Tribunal de Justiça do Ceará, a Qualificação Econômico-Financeira é um critério importante para a escolha da empresa vencedora, pois garante a solvência financeira e a capacidade de cumprimento do contrato firmado.

10.4.2. Certidão negativa de falência, concordata, recuperação judicial ou extrajudicial, expedida por quem de competência na sede da pessoa jurídica ou certidão negativa de execução patrimonial expedida no domicílio da pessoa física.

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALMEIDA LUNA, DIRETOR DE ENGENHARIA, MARIA NARCIZA CAVALCANTE GOMES, SERGIO MENDES DE CARVALHO, CRISTIANO BATISTA PACOSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para autenticidade deste documento, acesse o site: https://portaldeassinaturas.tjce.jus.br/validar e informe o processo 8521639-33.2023.8.06.0000 e o código A90613LT.

10.4.3. No caso de cooperativa, a mesma está dispensada da apresentação da Certidão exigida no subitem acima.

10.4.4. **BALANÇO PATRIMONIAL** e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira do licitante, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 meses da data de apresentação da proposta.

10.4.5. **COMPROVAÇÃO DA BOA SITUAÇÃO FINANCEIRA** atestada por documento, assinado por profissional legalmente habilitado junto ao Conselho Regional de Contabilidade da sede ou filial do licitante, demonstrando que a empresa apresenta índice de Liquidez Geral (LG) maior ou igual a 1,0 (um vírgula zero), calculada conforme a fórmula abaixo:

LG = (AC + ARLP)/(PC + PELP) ≥ 1,0

Onde:

LG – Liquidez Geral.

AC – Ativo Circulante.

ARLP – Ativo Realizável a Longo Prazo.

PC – Passivo Circulante.

PELP – Passivo Exigível a Longo Prazo.

10.4.6. No caso de sociedade por ações, o balanço deverá ser acompanhado da publicação em jornal oficial, em jornal de grande circulação e do registro na Junta Comercial.

10.4.7. No caso das demais sociedades empresárias, o balanço deverá ser acompanhado dos termos de abertura e de encerramento do Livro Diário - estes termos devidamente registrados na Junta Comercial - constando ainda, no balanço, o número do Livro Diário e das folhas nos quais se acha transcrito ou autenticada na junta comercial, devendo tanto o balanço quanto os termos ser assinados por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

10.4.8. No caso de empresa recém-constituída (há menos de 01 ano), deverá ser apresentado o balanço de abertura acompanhado dos termos de abertura e de encerramento devidamente registrados na Junta Comercial, constando no balanço o número do Livro e das folhas nos quais se acha transcrito ou autenticado na junta comercial, devendo ser assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

10.4.9. No caso de sociedade simples e cooperativa - o balanço patrimonial deverá ser inscrito no Cartório de Registro Civil de Pessoas Jurídicas assinado por contador registrado no

O original deste documento é eletrônico e foi assinado digitalmente por: juízes de direito SERGIO MENDES DE CARVALHO e LUIZA DENISE MARIA NARCISO GAGEN e CRISTIANO BATISTA PASSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento, acesse o site http://portaladoma.tjpe.jus.br/validardocumento e informe o processo 8521639-33.2023.8.06.0000 e o código A906I3LT.

Conselho Regional de Contabilidade e pelo titular ou representante legal da instituição, atendendo aos índices estabelecidos neste instrumento convocatório.

10.4.10. **PATRIMÔNIO LÍQUIDO MÍNIMO** não inferior a 10% da estimativa de custos, que deverá ser comprovado através da apresentação do balanço patrimonial.

10.4.11. A comprovação solicitada visa garantir que a CONTRATADA possua capacidade e porte suficiente para atender ao objeto desta contratação, bem como a capacidade financeira de sustentar suas atividades diante das oscilações de demandas que ocorrem durante a vigência do contrato.

10.5. Qualificação Técnica

10.5.1. Com o intuito de minimizar os riscos da contratação e alcançar os resultados esperados, é imprescindível que o LICITANTE possua capacidade técnica e de fornecimento para executar o objeto da licitação.

10.5.2. A exigência de comprovação de capacidade técnica relacionada ao objeto licitado se dá com fulcro no Art. 67 inciso I da Lei nº 14.133/21 e visa garantir que a LICITANTE já forneceu os serviços a serem contratados e, portanto, possui capacidade técnico-operacional para fornecê-lo adequadamente.

10.5.3. Conforme o Art. 67, inciso VI e § 2º da Lei nº 14.133/21: *§ 2º Observado o disposto no caput e no § 1º deste artigo, será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados.*; a licitante classificada deverá apresentar, para fins de habilitação, 1 (um) ou mais atestados de capacidade técnica que comprove a capacidade de fornecimento de serviços em até o mínimo 50% das demandas tecnológicas citadas nos itens 2, 3, 4 e na Tabela 3 do documento TRF ANEXO I. Os atestados de capacidade técnica devem atender os requisitos mostrados nos subitens 10.5.3.1 a 10.5.3.3, exclusivamente em seu nome, expedidos por pessoa jurídica de direito público ou privado, composto pela prestação de serviços SOC (Blue e Red Team) com coleta e análise de correlacionamento de informações de segurança e gestão de eventos (*Security Information and Event Management* - SIEM) em ambientes com as seguintes características:

10.5.3.1. A execução de serviços por no mínimo de 12 (doze) meses ininterruptos de serviços compostos por *Blue Team*, *Red Team* e Monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM.

10.5.3.2. No mínimo 500 (quinhentos) eventos por segundo (EPS) na ferramenta

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALCANTARA, SERGIO MENDONÇA DE ALVARENGA, LUIZA DE JESUS MARIA NARCISO, CLAUDEN DA CRUZ MADEIRA, CRISTIANO BATISTA PAULO SILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para autenticidade deste documento, consulte o site http://portaladoinfo.jfpe.jus.br/atendimento informe o processo 8521639-33.2023.8.06.0000 e o código A90613LT.

SIEM.

10.5.3.3. Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 100 (cem) ativos e 1.000 (mil) usuários.

10.5.4. A LICITANTE disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados.

10.5.5. Caso a LICITANTE não comprove as exigências previstas neste Termo de Referência por meio das documentações requeridas, será desclassificada.

10.5.6. O atestado deverá conter:

10.5.6.1. Razão Social, CNPJ e Endereço Completo da Empresa ou Órgão Emitente.

10.5.6.2. Razão Social da Contratada.

10.5.6.3. Número e vigência do contrato.

10.5.6.4. Objeto do contrato.

10.5.6.5. Local e Data de Emissão.

10.5.6.6. Assinatura do responsável pela emissão do atestado.

10.5.7. Tratando-se de empresa ou sociedade estrangeira em funcionamento no país, deve possuir Decreto de Autorização e Ato de Registro, ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

10.5.8. A não comprovação de alguma característica exigida, quando solicitada pelo Contratante, levará à desclassificação da proposta.

10.5.9. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da LICITANTE. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

10.5.10. O TJCE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas no Termo de Referência, podendo buscar por meios próprios ou exigir a apresentação de documentação complementar, tais como Notas Fiscais, Contratos, Atas do Pregão Original, entre outros, referente à prestação de serviços relativos aos atestados apresentados

10.5.11. É permitido o agrupamento de atestados de capacidade técnico-operacional, a fim de comprovar a experiência na prestação de serviços com características técnicas semelhantes ao objeto desta contratação.

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALBUQUERQUE LOPES, SERGIO MENDONÇA DE ARAUJO FILHO, DENISE MARIA NORONHA GOMES, CRISTIANO BATISTA PAROSILVA. Data da última assinatura: 14/11/2023 às 08:50:17.
Para autenticidade deste documento, acesse o site: https://portaldeassinaturas.tjce.jus.br/validar e informe o processo 8521639-33.2023.8.06.0000 e o código A906I3LT.

10.5.12. É possível aceitar a apresentação de atestados de serviços executados simultaneamente como comprovação do quantitativo mínimo do serviço, uma vez que essa situação é equivalente, em termos de comprovação da capacidade técnico-operacional, a uma única contratação.

10.5.13. Os atestados devem estar relacionados a serviços realizados no contexto de sua atividade econômica principal ou secundária, conforme descrito no contrato social atualizado.

10.5.14. A comprovação de capacidade técnica estará sujeita à confirmação da veracidade de suas informações através de possíveis diligências, conforme prescreve o art. 59, § 2º, da Lei 14.133/21.

10.5.15. Por fim, caso a empresa esteja sob falência, concurso de credores, dissolução ou liquidação, deve apresentar Plano de Recuperação Judicial, devidamente homologado. Se nessas condições e, ainda, sendo formada em consórcio de empresas, esta não deverá ser controladora, coligada ou subsidiária entre si, devendo, da mesma forma, apresentar Plano de Recuperação Judicial, devidamente homologado.

11. GARANTIA CONTRATUAL

11.1. A CONTRATADA deverá entregar ao Gerente de Contratação do objeto, que submeterá à Coordenadoria Central de Contratos e Convênios do TJCE, no prazo prescrito no art. 96 da Lei n.º 14.133/2021, a título de garantia, a quantia equivalente a 5% (cinco por cento) do valor global da contratação, cabendo-lhe optar dentre as modalidades previstas no art. 96, Lei n.º 14.133/2021.

11.1.1. A garantia será devolvida à CONTRATADA somente depois do cumprimento integral das obrigações assumidas, inclusive recolhimento de multas e satisfação de prejuízos causados ao CONTRATANTE.

11.1.2. Será exigida do licitante vencedor a indicação na sua proposta a modalidade da garantia escolhida, a fim de possibilitar a contagem do prazo de acordo com cada modalidade.

11.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

11.2.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas.

11.2.2. As multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA.

11.2.3. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

11.3. A contratada terá o prazo mínimo de 1 (um) mês, contando do recebimento do termo de

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALSSERGIO MENDONÇA DE ALMEIDA, FULVIO DEUSIRE MARIA NARCISO CALSEN DA CRISTIANO BATISTA PACOSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para autenticidade deste documento, acesse o site: https://portaladoma.tjce.jus.br/sgd/validacaoDocumento.jsp, informe o processo 8521639-33.2023.8.06.0000 e o código A90613LT.

intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pela modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

11.3.1. A apólice deverá seguir as regras estatuídas na Circular Susep nº 662, de 11 de abril de 2022, quando da escolha por parte do licitante vencedor da modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

11.3.2. O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas, conforme inciso II do artigo 97 da Lei Nº 14.133/21.

11.3.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados neste documento, observada a legislação que rege a matéria.

11.4. A contratada terá o prazo mínimo de 10 (dez) dias corridos, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pelas demais modalidades previstas no § 1º do art. 96, da Lei Nº 14.133/21.

11.4.1. A garantia em dinheiro deverá ser efetuada em instituição bancária indicada pelo CONTRATANTE, com correção monetária, em favor do CONTRATANTE.

11.4.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

11.4.3. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.5. A garantia deverá ter validade durante a execução do contrato de 90 (noventa) dias após término da vigência contratual, devendo acompanhar as modificações referentes ao valor e à vigência desta mediante a complementação da caução ou emissão do respectivo endosso pela seguradora ou instituição bancária fiadora.

11.5.1. O prazo para complementação da caução ou emissão do endosso da garantia referente aos aditivos contratuais deverá seguir os mesmos prazos estabelecidos nos subitens 11.3 e 11.4.

11.6. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento de multas, ela deve ser complementada no prazo de até 10 (dez) dias úteis, contados da solicitação do CONTRATANTE, a partir do qual se observará o disposto abaixo:

11.6.1. 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.

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

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALMEIDA SERGIO MENDES DE CARVALHO FILHO, DENISE MARIA NARCISO GALEN DA CRUZ, CRISTIANO BATISTA PACOSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para autenticar a autenticidade deste documento, acesse o site http://portaladoma.tjpe.jus.br/atendimento/informe o processo 8521639-33.2023.8.06.0000 e o código A906I3LT.

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

11.8. A garantia será considerada extinta:

11.8.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro ou títulos da dívida pública, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

11.8.2. No prazo de 90 (noventa) após o término da vigência, caso o CONTRATANTE não comunique a ocorrência de sinistros.

11.9. A ausência de prestação da garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa e rescisão unilateral do contrato administrativo.

12. VIGÊNCIA CONTRATUAL

12.1. A vigência do contrato inicia na data de sua assinatura vigorará por até 36 (trinta e seis) meses, podendo ser prorrogado até limite permitido pela Lei 14.133/21.

12.2. A escolha do prazo de 36 (trinta e seis) meses de vigência baseia-se não somente no investimento, mas também na continuidade e no desempenho de funções de segurança da informação do TJCE, agregado à possibilidade de renovação dos itens de serviço, até o limite permitido pela atual legislação, desde que se comprove vantajoso ao TJCE.

12.3. Além disso, no custo administrativo de um processo licitatório, já que quanto maior o número de procedimentos, maior o gasto da administração, considerando contratações de serviços continuados, como o que aqui se trata.

12.4. O prazo dilatado permitirá obtenção de ganho de escala, reduzindo o grau de incerteza da contratação e consequentemente melhores preços para a Administração.

12.5. Ademais, é maior a atratividade do certame pelo mercado, por meio de uma maior diluição dos custos dos serviços oferecidos pela contratada durante o lapso temporal do contrato, favorecendo a Administração em termos de economicidade e ampliação da competitividade.

12.6. Como também está alinhada ao padrão praticado no mercado, como pode ser verificado nas contratações públicas similares (disponível no item 2.6.2).

12.7. Por se tratar de um objeto de execução crítica e de tamanha importância para o judiciário cearense, como também foi definida acima, a importância da solução a ser adquirida, vemos também, a importância e quão crítica é a perfeita execução do objeto e a relevância de uma

O original deste documento é eletrônico e foi assinado digitalmente por: tjce.jus.br:SERGIO MENDES DE ARAUJO FILHO:PEANA MARIA NARCISO GOMES:CRISTIANO BATISTA PACOSILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento acesse o site: https://portaladoministrativo.tjce.jus.br/portaldeprocessos e informe o processo 8521639-33.2023.8.06.0000 e o código A90613LT.

manutenção e suporte contínuo. Garantindo qualidade e eficiência no funcionamento da Solução, bem como a facilidade e eficiência na gestão do contrato para a Administração.

12.8. A contratação em tela envolve serviços de natureza continuada, necessários à conservação do futuro patrimônio público, objeto desta contratação acima descrito, e ao bom andamento das atividades judiciárias e administrativas desenvolvidas pelo Poder Judiciário Cearense e, consequentemente, para toda a sociedade de modo geral.

12.9. Os serviços relacionados à manutenção integral de todos os componentes da solução e seu funcionamento é que vinculam-se à indispensável continuidade da sua prestação, pois os referidos serviços objetivam à manutenção profissional, eficiente, competente, capacitada e confiante da infraestrutura de processamento de dados, logrando evitar transtornos relacionados à solução de continuidade na prestação do objeto contratual. Além dessa essencialidade do serviço em pleno funcionamento, a ideia de manter a solução sob constante cuidado operacional e funcionando ininterruptamente (habitualidade), relaciona-se com a necessidade monitorar e responder a incidentes cibernéticos, possibilitando, assim, condições adequadas ao exercício das atividades-fim da Corte de Justiça do Estado do Ceará, de seus servidores, dos colaboradores e demais jurisdicionados.

12.10. A caracterização de um serviço como contínuo requer a demonstração de sua essencialidade e habitualidade para o contratante, conforme explicação supra. Sabe-se que a essencialidade se atrela à necessidade de existência e manutenção do contrato, pelo fato de eventual paralisação da atividade contratada implicar em prejuízo ao exercício das atividades da Administração contratante, condição integramente esclarecida no item anterior. Já a habitualidade ficou configurada pela necessidade desta atividade ser prestada mediante contratação de terceiros de modo permanente, ou seja, estendendo-se por mais de um exercício financeiro de forma contínua.

12.11. Atenta-se, nesse sentido, ao entendimento da Corte de Contas da União, quando em seu Acórdão n° 132/2008, da Segunda Câmara, sob relatoria do Ministro Aroldo Cedraz, prescreve que contratos dessa natureza intentam "manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional".

12.12. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, suporte e garantia inerentes a solução a ser adquirida, sobretudo os utilizados pelo TJCE, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos.

O original deste documento é eletrônico e foi assinado digitalmente por: JOSE LUIS DE ALMEIDA LUNA, DENISE MARIA NARCISO CARNEIRO, CRISTIANO BATISTA PAULA SILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento, acesse o site: http://portaladministrativo.tjce.jus.br/sgpe/acesse.jsp e informe o nº do processo 8521639-33.2023.8.06.0000 e o código A90613LT.

12.13. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, de suporte e de garantia, inerentes à solução a ser adquirida, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual, em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos, e a imperiosidade da sua prestação ininterrupta em face do desenvolvimento habitual das atividades administrativas, sob pena de prejuízo ao interesse público, denota-se necessária a contratação pelo tempo indicado, conforme descrito neste documento.

12.14. Diante do exposto, considera-se de extrema relevância para a Administração a contratação do objeto em tela, entendendo imprescindível a vigência do termo de contrato por até 36 (trinta e seis) meses, contados da data de emissão do Termo de Recebimento Definitivo.

Equipe de Planejamento da Contratação

Max Eduardo Vizcarra Melgar - 48994 Integrante Técnico	**Fábio de Carvalho Leite – 9594** Integrante Administrativo	**Heldir Sampaio Silva - 9630** Integrante Demandante
Cristiano Henrique Lima de Carvalho – 5198 Área Demandante		

O original deste documento é eletrônico e foi assinado digitalmente por: juiz de direito SERGIO MENDES DE ALMEIDA, LUIZA DENISE MARIA NARCISO GAGEN DA SILVEIRA, MARIA NARCISO GAGEN DA SILVEIRA, CRISTIANO BAUNGARTEN PASSOS, LUCIANA DA CUNHA E SILVA. Data da última assinatura: 14/11/2023 às 09:50:17.
Para verificar a autenticidade deste documento, acesse o site: https://pje.tjpa.jus.br/pje/ea/consultaDocumento.jsf informe o processo 8521639-33.2023.8.06.0000 e o código A906I3LT.

13. APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Licitação para iniciação de procedimento licitatório, segundo o art. 38 da Lei nº 8.666 de 21 de junho de 1993.

Autoridade Competente

Denise Maria Norões Olsen – 24667

Área de Tecnologia da Informação

Fortaleza, 26 de setembro de 2023.

O original deste documento é eletrônico e foi assinado digitalmente por usuários de sistemas do TJCE, nos termos da Lei 11.419/2006 e da Resolução TJPGE 2.000/2019.
Para verificar a autenticidade deste documento, acesse o site: https://pje.tjce.jus.br/pje/atividade-usuario/validarDocumento e informe o processo 8521639-33.2023.8.06.0000 e o código A906I3LT.
DENISE MARIA NORONES OLSEN:24667:DENISE MARIA NORONES OLSEN:24667 e CRISTIANO BATISTA PAULO SILVA: Data da última assinatura: 14/11/2023 às 09:50:17.
SERGIO MENDES DE ALMEIDA FILHO:8:SERGIO MENDES DE ALMEIDA FILHO:8 e CRISTIANO BATISTA PAULO SILVA: Data da última assinatura: 26/09/2023 às 12:48:55.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA 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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
329

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
326

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
324

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
328

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
320

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
328

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
329

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
330

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e BAIXOU DOCUMENTO EM 12/09/2023 08:50:45.
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código 23091215334.

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
332

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
336

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.

2.4.3.1 Deve contar com, pelo menos, uma das seguintes certificações: Certified Information Systems Auditor (CISA); Certified Incident Handler (GCIH); CompTIA CySA+.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
334

3. 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.

.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
338

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,

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
330

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:

3.3.5.2.2.1. 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.

3.3.5.2.2.2. Coleta ativa, com a utilização de, no mínimo, as seguintes técnicas: Port scanning (Mapeamento de rede); Varredura de vulnerabilidade.

3.3.5.2.2.3. 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;

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
330

Vulnerabilidades de Médio Risco; Vulnerabilidades de Baixo Risco; Informações a serem aplicadas na fase de ataques.

3.3.5.2.2.4. 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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
338

(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:

3.3.5.3.7.1. Padrões para testes de gerenciamento de configuração: OWASPCM001, OWASPCM002, OWASPCM003, OWASPCM004, OWASPCM005, OWASPCM006, OWASPCM007, OWASPCM008.

3.3.5.3.7.2. Padrões para testes de autenticação: OWASPAT001, OWASPAT002,

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

OWASPAT003, OWASPAT004, OWASPAT005, OWASPAT006, OWASPAT007, OWASPAT008, OWASPAT009 e OWASPAT010.

3.3.5.3.7.3. Padrões para testes de gerenciamento de sessão: OWASPSM001, OWASPSM001, OWASPSM002, OWASPSM003, OWASPSM004, OWASPSM005.

3.3.5.3.7.4. Padrões para testes de autorização: OWASPAZ001, OWASPAZ002 e OWASPAZ003.

3.3.5.3.7.5. Padrão para testes de negócio lógico: OWASPBL001.

3.3.5.3.7.6. Padrões para testes de validação de dados: OWASPDV001; OWASPDV002, OWASPDV003, OWASPDV004, OWASPDV005, OWASPDV006, OWASPDV007, OWASPDV008, OWASPDV009, OWASPDV010, OWASPDV011, OWASPDV012, OWASPDV013, OWASPDV014, OWASPDV015 e OWASPDV016.

3.3.5.3.7.7. Padrões para testes de negação de serviços: OWASPDS001, OWASPDS002, OWASPDS003, OWASPDS004, OWASPDS005, OWASPDS006, OWASPDS007 e OWASPDS008.

3.3.5.3.7.8. Padrões para testes de serviços web: OWASPWS001, OWASPWS002,

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
340

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
344

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:

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
342

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+.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
348

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
347

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
348

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
358

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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).

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
350

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
354

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
352

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
358

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).

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
354

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
358

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
350

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
360

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
368

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
360

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:

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
362

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
368

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
364

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
368

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.

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]
360

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]

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

O original deste documento é eletrônico e foi assinado digitalmente por tjce.jus.br e [illegible]
Para verificar a autenticidade desta cópia impressa, acesse o site http://portaladmin.tjce.jus.br/atendimento e informe o processo 8521639-33.2023.8.06.0000 e o código [illegible]