Termo de Referência Nº 161/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

TERMO DE REFERÊNCIA / PROJETO BÁSICO

REGISTRO DE PREÇO PARA AQUISIÇÃO DE SOLUÇÃO AVANÇADA DE ENDPOINT

1. FUNDAMENTO LEGAL

1.1. Legislação Federal/Nacional: Lei nº 10.520/2002, Decretos nº 3.555/2000, nº 10024/2019, nº 7.892/2013 e suas alterações; Lei Complementar nº 123/2006 e subsidiariamente, Lei nº 8.666/93 e Lei nº 8.078/1990, Resolução Nº 182/2013 do Conselho Nacional de Justiça e outras normas aplicáveis ao objeto deste certame.

1.2. Legislação do Estado do Piauí: Decreto nº 11.319/04 (Regulamento do SRP do Governo do Estado do Piauí), Resolução TJ/PI nº 19/2007, Portaria nº 168/2011/TJPI, **Portaria TJPI Nº 2.503/2016,** que dispõe sobre as diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelo TJ/PI e outras normas aplicáveis ao objeto deste certame e, ainda, pelo estabelecido no instrumento convocatório que permear o referido certame.

1.3. A licitante deverá se credenciar no sítio www.comprasgovernamentais.gov.br, sistema "Pregão Eletrônico", para participar da Licitação.

2. OBJETO (art. 18, §3, I)

2.1. Contratação via **Registro de Preços** de **Solução de Proteção avançada de endpoints Palo Alto Cortex XDR e serviços de implantação e configuração da solução (incluindo Hands On)**, com direito de atualização e suporte, em português do Brasil, por meio de licenças de subscrição por *endpoint.*

2.2. Havendo divergências entre as especificações dos itens constantes do Termo de Referência e as do sistema de pregão eletrônico prevalecerão as primeiras.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Motivação da contratação (art. 18, §3, II, a)

O Tribunal de Justiça do Estado do Piauí utiliza atualmente em seu parque computacional diversas ferramentas antivírus, que tem por objetivo principal a proteção contra ataques virtuais e infecções de programas maliciosos. No entanto, estas soluções se restringem a ferramentas gratuitas, baixadas da Internet e que são projetadas para uso doméstico, sempre apresentando alguma limitação, seja em termos de gerência, visibilidade, licenciamento ou funcionalidade.

Além disso, são antivírus de fabricantes diferentes, o que dificulta sua gerência e manutenção. Este cenário está longe de ser o ideal para uma proteção aprimorada de um ambiente corporativo, sobretudo de um órgão da justiça.

O que se propõe é a aquisição de uma solução de proteção de fabricante único, que possa ser gerenciada de modo centralizado, que possua todos os módulos e funcionalidades disponíveis habilitados e atuantes, além de estar licenciada para uso corporativo em todo o ambiente computacional do TJPI.

O objeto desta contratação, portanto, é a aquisição de uma solução de segurança abrangente, com **características estendidas de detecção e resposta a incidentes de segurança,** conhecidas no mercado de segurança como **XDR** (e**X**tended **D**etection and **R**esponse), proveniente da sua sigla no idioma Inglês, onde o "D" significa Detecção, o "R" Resposta e o grande diferencial está no "X", que significa qualquer fonte de dados, não se limitando somente ao endpoint, como é o caso do EDR (**E**ndpoint **D**etection and **R**esponse). Com esta solução de segurança totalmente operacional o ambiente computacional o TJPI terá proteção aprimorada contra os mais variados tipos de *malwares* e técnicas utilizadas pelos atacantes, já que a solução terá uma visão ampla e unificada sobre as várias camadas de segurança gerenciadas por ela, abrangendo inicialmente as camadas de Endpoint e Rede, mas possibilitando sua expansão para outras camadas, como o E-mail e Nuvem, por exemplo.

3.2. Objetivos a serem alcançados (art. 18, §3, II, b)

- Prover uma análise estendida das camadas de rede e endpoint;
- Permitir a integração de outras camadas de segurança dentro da mesma plataforma;
- Oferecer mecanismos de detecção e resposta aos incidentes cibernéticos;
- Complementar a proteção de segurança da solução NGFW já instalada no TJPI;
- Proteger as estações de trabalho dos mais variados tipos de malware;
- Oferecer proteção contra exploração de vulnerabilidades;
- Permitir auditoria dos eventos ocorridos;
- Proteger informações sensíveis no endpoint e na rede.

3.3. Benefícios diretos e indiretos (art. 18, §3, II, c)

Com a contratação em epígrafe são esperados os seguintes resultados:

- Gerenciamento unificado e proteção avançada da solução de proteção;
- Proteção contra ameaças virtuais para os dispositivos conectados na rede corporativa deste TJPI;
- Defesa proativa e responsiva de ataques virtuais;
- Salvaguarda das informações que tramitam nas estações de trabalho e servidores deste Tribunal.

3.4. Alinhamento estratégico (art. 18, §3, II, d)

A presente demanda está alinhada ao PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PDTI TJPI 2021-2022 (SEI 2414707) e a ESTRATÉGIA NACIONAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PODER JUDICIÁRIO - ENTIC-JUD 2021-2026:

ALINHAMENTO - PDTI TJPI 2021-2022 (SEI 2414707)
8.2.4. Objetivo Estratégico 06: Aprimorar a Segurança da Informação e a Gestão de Dados

AÇÃO	DESCRIÇÃO
Aquisição de Licenciamento Endpoint (antivírus)	Aquisição de Solução de proteção antivírus adequado ao ambiente corporativo onde, diferentemente do uso doméstico, existem constantes e complexas trocas de informações entre os dispositivos e serviços de infraestrutura de TIC, dentro de uma mesma rede. A solução deve ter características para poder proteger de forma completa as estações de trabalho da rede.

ALINHAMENTO - ENTIC-JUD 2021 -2026		
4.1.2 Processos internos	**OE 6**	**Iniciativa**
	Aprimorar a Segurança da Informação e a Gestão de Dados	Melhorar os avanços voltados para a Segurança da Informação e dados pessoais frente aos mais diversos desafios, fazendo-se valer principalmente das vantagens oriundas da utilização de Inteligência Artificial e demais soluções disruptivas de TIC.

Além disso, a Manifestação SEI 2562395 corroborada com o Despacho SEI 2598287, ambos no Processo SEI Nº 21.0.000006549-5 preveem "a realização do remanejamento interno para atender as demandas de TI na rubrica orçamentária 449040 - Serviços de Tecnologia da Informação e Comunicação, conforme consta na NC - Nota de Crédito (2598282)", dentre elas a necessária para o atendimento da Aquisição de Licenciamento EndPoint.

3.5. Referência aos estudos preliminares (art. 18, §3, II, e)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda – DOD Nº 25/2021 (SEI 2324888) e os Estudos Preliminares Nº 47/2021 (SEI 2371110) elaborados pelo setor de Aquisições e Contratações de Soluções de TIC da STIC - ACSTIC, ambos devidamente protocolados no Processo SEI Nº 21.0.000032562-4.

3.6. Relação entre a demanda prevista e a contratada (art. 18, §3, II, f)

Nome da Solução	Item	Quantidade a ser Registrada	Quantidade a ser contratada de Imediata
Solução de Proteção Avançada de Endpoints Palo Alto Cortex XDR	Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	4500	3840
	Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	4500	3840
	Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro (**incluindo Hands On)**	1	1

O quantitativo descrito acima é estimado. Poderá sofrer alteração dependendo da data da contratação, e do orçamento disponível.

3.7. Análise do mercado de TIC (art. 18, §3, II, g)

Os programas antivírus estão disponíveis no mercado de TIC há muito tempo, mas evoluem constantemente para fazer frente à crescente variedade de ameaças. Diversas abordagens podem ser adotadas para proteger as várias camadas de segurança utilizadas.

Uma delas é a de criar mecanismos alternativos à simples identificação das ameaças: proteção baseada em assinaturas, controle de aplicações e análise heurística (que bloqueia a execução de códigos com comportamento diferente do esperado). As soluções tradicionais já não são tão eficazes para um ambiente corporativo.

Outra abordagem é a oferta de soluções de segurança mais abrangentes, como as ferramentas de EDR, NDR e XDR, sendo vendidas na forma de suítes integradas que protegem contra uma grande variedade de ameaças virtuais, exploração de vulnerabilidades, investigação e resposta à incidentes de segurança e perda de dados, dentre outros.

- **Antivírus tradicional:** Trabalha com vacinas, produzidas pelos fabricantes quando estes identificam as primeiras infecções. Após a vacina ser feita pelo fabricante a solução é atualizada e passa a conseguir bloquear as ameaças que constam no seu banco de dados.
- **Antivírus com EDR** (**E**ndpoint **D**etection and **R**esponse)**:** Acrescentam a Detecção e Resposta aos incidentes, permitindo investigar o incidente logo após a geração dos eventos. Também trabalham com inteligência artificial e aprendizado de máquina. Contudo sua abrangência e visibilidade **é limitada à camada dos Endpoints** (Abrange somente os dispositivos protegidos, como Estações de trabalho, Smartphones e Tablets, por exemplo).
- **Soluções de NDR:** Uma ferramenta de **NTA** (Analisador de Tráfego de Rede ou **N**etwork **T**raffic **A**nalysis, na sigla em inglês) também conhecida como **NDR** (Detecção e Resposta de Rede ou **N**etwork **D**etection and **R**esponse, na sigla em inglês), por trazer consigo a inteligência da Detecção e Resposta. Possui visibilidade e abrangência limitada **por atuar somente na camada da rede.**
- **Proteção de endpoint XDR:** Possui uma **abrangência estendida** (e**X**tended **D**etection and **R**esponse) pois permite correlacionar eventos de diversas camadas de segurança, **como Endpoint, Rede, E-mail e Nuvem**, além de gerenciar as várias camadas de segurança dentro de uma **console de gerenciamento única**.

As soluções disponíveis no mercado de proteção de endpoints são numerosas e bastante variadas, indo desde antivírus gratuitos, de aplicação doméstica, passando por soluções comerciais com e sem detecção e resposta a incidentes (EDR), chegando a soluções mais completas para ambientes corporativos, integrando diversas camadas de segurança como rede, firewall, IoT, nuvem e Endpoints (XDR).

3.8. Natureza do objeto (art. 18, §3, II, h)

O objeto a ser contratado enquadra-se na categoria de serviços comuns de que tratam a Lei nº 10.520/02 e os Decretos nº 3.555/00 e nº 10024/2019, por possuir padrões de desempenho e características gerais e específicas que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

3.9. Parcelamento do objeto (art. 18, §3, II, i)

Considerando razões de padronização e compatibilidade, a contratação dos itens que compõem o objeto pretendido deverá ser realizada em **lote único**, pois os itens relativos às licenças e aos **serviços de implantação e configuração da solução (incluindo Hands On)** guardam interdependência entre si, além de serem da mesma natureza, estando diretamente conformes ao princípio da integração dos serviços de Tecnologia da Informação do TJPI.

O agrupamento dos itens em lote único não comprometerá a competitividade do certame, uma vez que há no mercado número suficiente de fornecedores capazes de executar o objeto em sua totalidade.

3.10. Forma e critério de seleção do fornecedor (art. 18, §3, III, j)

Tratando-se de lote único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade entre os itens constantes do lote.

Considerando que os serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a utilização do **sistema de pregão na sua modalidade eletrônica do tipo menor preço**.

Os seguintes documentos servirão como condição para aceite da proposta:

i. Especificação clara, completa e minuciosa do produto cotado, informando a marca, o modelo e o fabricante, bem como a indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência, pontuando em forma de planilha cada exigência do edital com sua respectiva comprovação, que deve conter uma ou mais das seguintes:

- Indicação da página/item do manual/*datasheet*;
- URL;
- Seção/subseção ou número de item de página WEB;
- Print de tela da solução;
- Imagem ou vídeo que demonstre a funcionalidade;
- Outra comprovação, desde que seja oficial do fabricante do produto ofertado.

a) Entende-se por documento (s) a documentação técnica oficial do fabricante do produto ofertado, seja em meio eletrônico ou materializada em papel;

b) Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.

ii. Caso a licitante não seja o próprio fabricante, deverá apresentar documento emitido pelo fabricante dos produtos, que comprove que a licitante é um parceiro oficial habilitado a comercializar seus produtos. A implantação e configuração da solução, deverá ser feita por profissional certificado pelo fabricante.

3.10.1 PARA A HABILITAÇÃO EXIGIR-SE-Á DOS INTERESSADOS DOCUMENTAÇÃO RELATIVA A:

- habilitação jurídica;
- qualificação técnica;
- qualificação econômico-financeira;
- regularidade fiscal e trabalhista;
- cumprimento do disposto no inciso XXXIII do art. 7o da Constituição Federal. (Incluído pela Lei nº 9.854, de 1999)

3.11. Documentos relativos à QUALIFICAÇÃO TÉCNICA

3.11.1 Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado que comprovem que a licitante já prestou serviços semelhantes ao objeto ora licitado.

3.11.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

3.11.2.1. Os atestados deverão referir-se aos serviços fornecidos no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

3.11.2.2. Considerar-se-ão fornecimentos de serviços semelhantes aqueles de natureza e complexidade similar ao objeto e compatível em características, quantidades e prazos de execução relacionada com o objeto desta licitação, conforme Acórdão nº 914/2019-Plenário TCU;

3.11.2.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, no mínimo, 12 (doze) meses do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG Nº 5, de 2017;

3.11.2.4. Não serão aceitos atestados decorrentes de contratos em andamento, exceto quando se tratar de serviços executados de forma contínua, conforme definição do Art. 57, II da Lei nº 8.666/93;

3.11.3. Os produtos fornecidos, objeto desta licitação, deverão atender aos padrões de qualidade e estarem em conformidade com a legislação vigente no país;

3.11.4. Em todos os casos o pregoeiro poderá diligenciar a fim de comprovar o atendimento dos requisitos, antes de proceder à desclassificação do licitante;

3.11.5. Quando solicitado pelo pregoeiro, a empresa deverá disponibilizar todas as informações necessárias à comprovação da legitimidade do atestado entregue, apresentando, dentre outros documentos, cópia dos contratos, notas fiscais e dos documentos do responsável técnico pela execução do contrato, com registro no conselho de classe, conforme o caso;

3.12. Impacto ambiental (art. 18, §3, III, k)

Não haverá alteração das propriedades físicas, químicas e biológicas do meio ambiente, causada por qualquer forma de matéria ou energia resultante das atividades humanas que, direta ou indiretamente afetam as condições estéticas e sanitárias do meio ambiente. Dentro do quadro existente a melhoria das condições ambientais será trazida pela destinação adequada dos equipamentos e componentes não utilizados, descarte de resíduos eletrônicos e adoção de critérios de sustentabilidade evitando-se o consumo excessivo de energia elétrica, além de limitar o uso de materiais poluentes (graxas, óleos, gases, etc.).

3.13. Conformidade técnica e legal (art. 18, §3, III, l)

Este procedimento obedecerá, integralmente, à Constituição Federal de 1988, à Lei Federal n.º 10.520/2002, à Resolução do CNJ n.º 182 de 2013, às disposições contidas na Lei Federal n.º 8.666 de 1993, e legislações correlatas bem como suas respectivas alterações posteriores.

4. Obrigações Contratuais (art. 18, §3, III, m)

4.1. Das obrigações do CONTRATANTE

Além das obrigações resultantes da observância da Lei 8.666/93, a CONTRATANTE deverá:

4.1.1. Acompanhar, atestar e remeter nas notas fiscais/faturas a efetiva entrega do objeto;

4.1.1.1. Validar e aprovar os produtos e serviços liberados.

4.1.1.2. Receber o objeto de acordo com as disposições deste Termo de Referência.

4.1.1.3. Definir o Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, o Fiscal Administrativo, responsáveis por fiscalizar a execução contratual, conforme disposto no Art. 16 da Resolução 182/2013 do Conselho Nacional de Justiça – CNJ.

4.1.2. Efetuar o pagamento do material, nas condições e preços pactuados, dentro do prazo fixado neste contrato, após a entrega da documentação pelo Fiscal de Contrato à SOF.

4.1.2.1. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência;

4.1.3. Comunicar à CONTRATADA, o mais prontamente possível, qualquer anormalidade observada no fornecimento do objeto requisitado que possa comprometer a tempestividade, a qualidade e a eficácia do uso a que se destina;

4.1.4. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA.

4.1.5. Fornecer, a qualquer tempo e com a máxima presteza, mediante solicitação escrita da CONTRATADA, informações adicionais, dirimir dúvidas e orientá-la em todos os casos julgados necessários;

4.1.6. Manter os contatos com a CONTRATADA por escrito, ressalvados os entendimentos verbais determinados pela urgência que, posteriormente, devem ser confirmados por escrito no prazo de até 72 (setenta e duas) horas.

4.1.7. A CONTRATANTE não aceitará, sob nenhum pretexto, transferência de responsabilidade da CONTRATADA para terceiros, sejam fabricantes, representantes ou quaisquer outros.

4.1.8. Permitir acesso dos empregados da CONTRATADA às dependências do TJPI para entrega do objeto.

4.1.8.1. Fornecer a infraestrutura necessária para a realização das atividades que devam ser executadas em suas instalações conforme as especificações estabelecidas neste Termo de Referência.

4.1.8.2. Providenciar o acesso controlado aos recursos de TIC do TJPI para os profissionais da CONTRATADA durante a fase de execução do objeto, caso necessário.

4.1.9. Supervisionar e gerenciar os procedimentos a serem realizados pelos fiscais de contrato.

4.1.10. Exigir o afastamento de qualquer funcionário ou preposto da CONTRATADA que venha a causar embaraço ou que adote procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas.

4.1.11. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

4.1.12. Aplicar à CONTRATADA as penalidades regulamentares e contratuais.

4.2. Das obrigações da CONTRATADA

Além das obrigações resultantes da observância da Lei 8.666/93, a CONTRATADA deverá:

4.2.1. Fornecer o(s) objeto(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos, na Proposta e no Contrato.

4.2.2. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos vinculados ao fornecimento, dentro dos prazos e condições estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.

4.2.3. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato.

4.2.4. Atender prontamente às solicitações do Tribunal de Justiça do Estado do Piauí no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do Gestor do Contrato.

4.2.5. Seguir as instruções e observações efetuadas pelo Gestor do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, partes do objeto em que se verificarem vícios, defeitos ou incorreções.

4.2.6. Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução contratual.

4.2.7. Assumir responsabilidade irrestrita sobre a totalidade do fornecimento de insumos e serviços associados ao fornecimento do objeto.

4.2.8. Indicar, formalmente, preposto apto a representá-la junto a CONTRATANTE que deverá responder pela fiel execução do Contrato.

4.2.9. Cuidar para que o preposto indicado mantenha permanente contato com o Gestor do Contrato e adote as providências requeridas pelo TJPI, além de comandar, coordenar e controlar a atuação deste quando da execução do objeto.

4.2.10. Prestar todos os esclarecimentos que forem solicitados pelo Tribunal de Justiça do Piauí, devendo, ainda, atender prontamente às reclamações.

4.2.11. Comunicar, imediatamente e por escrito, qualquer anormalidade ou problema detectados, prestando à CONTRATANTE os esclarecimentos necessários.

4.2.12. Manter, durante a execução contratual, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para o fornecimento do objeto.

4.2.13. Assumir inteira responsabilidade técnica e operacional pelo fornecimento do objeto e os serviços diretamente vinculados, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na execução.

4.2.14. Responder integralmente por quaisquer perdas ou danos causados à CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução contratual, independentemente de outras cominações contratuais ou legais a que estiver sujeito.

4.2.15. Arcar com todas as despesas decorrentes de transporte, diárias, tributos, seguros, alimentação, assistência médica e de pronto socorro, ou qualquer outra despesa de seus empregados.

4.2.16. Arcar com o pagamento de todas as despesas decorrentes do fornecimento do objeto, incluindo as despesas definidas em leis sociais, trabalhistas, comerciais, tributárias e previdenciárias, impostos e todos os custos, insumos e demais obrigações legais, inclusive todas as despesas que onerem, direta ou indiretamente, o objeto ora contratado, não cabendo, pois, quaisquer reivindicações da CONTRATADA, a título de revisão de preço ou reembolso.

4.2.17. Promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários à execução contratual, até as instalações da CONTRATANTE.

4.2.18. Respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no Estado do Piauí, bem como atentar para as regras de cortesia onde sejam executados os serviços.

4.2.19. Substituir qualquer de seus profissionais cuja qualificação, atuação, permanência ou comportamento durante a execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público por outro de qualificação igual ou superior, sempre que exigido pela CONTRATANTE.

4.2.20. Garantir a execução dos serviços vinculados à execução contratual, mantendo equipe adequadamente dimensionada para tanto, sem ônus adicionais para o órgão contratante.

4.2.21. Zelar pela boa e completa execução dos serviços vinculados à execução contratual, mantendo recursos técnicos e humanos necessários para evitar a interrupção indesejada dos mesmos.

4.2.22. Facilitar, por todos os meios a seu alcance, a ampla ação fiscalizadora do órgão contratante, atendendo prontamente às observações e exigências que lhe forem dirigidas.

4.2.23 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, especialmente em relação a: dados, informações, regras de negócios, documentos, e outros.

4.2.24. Honrar os honorários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços vinculados ao fornecimento, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vales-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhe defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para a CONTRATANTE.

4.2.25. Responder, perante a CONTRATANTE e terceiros, pela conduta dos seus empregados designados para execução do objeto do contrato, com o propósito de evitar condutas que possam comprometer a segurança ou a credibilidade da CONTRATANTE.

4.2.26. Adotar regras de vestimenta para seus profissionais adequadas com o ambiente do órgão, com trajes em bom estado de conservação e portando crachá de identificação funcional com foto e nome visível, arcando com o ônus de sua confecção.

4.2.27. Utilizar as melhores práticas de mercado no gerenciamento de recursos humanos e supervisão técnica e administrativa para garantir a qualidade da execução do objeto e o atendimento das especificações contidas no Contrato, Edital e seus Anexos.

4.2.28. Cumprir e fazer cumprir por seus profissionais as normas e procedimentos estabelecidos na Política de Segurança da Informação da CONTRATANTE.

4.2.29. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do órgão contratante, afixando placas de controle patrimonial, selos de segurança, entre outros pertinentes, e responsabilizar-se por estes.

4.2.30. Manter os contatos com a CONTRATANTE sempre por escrito, ressalvados os entendimentos verbais determinados pela urgência na execução do Contrato que, posteriormente, devem sempre ser confirmados por escrito, dentro de até 72 (setenta e duas) horas, a contar da data de contato;

4.2.31. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial do contrato.

4.2.32. Comunicar à CONTRATANTE, com antecedência de 48 (quarenta e oito) horas os motivos que eventualmente impossibilitem a prestação dos serviços no prazo estipulado, nos casos em que houver impedimento justificado para funcionamento normal de suas atividades, sob a pena de sofrer as sanções da Lei 8.666/93.

4.2.33. Vincular-se ao que dispõe a lei nº 3.078, de 11/09/90 (Código de Proteção de Defesa do Consumidor).

4.2.34. São expressamente vedadas à CONTRATADA:

I. A contratação de servidor pertencente ao quadro de pessoal do TJ/PI, durante o período de fornecimento.

II. A subcontratação total do objeto do Contrato. E sendo parcial, somente para assistência técnica de garantia e implantação da solução, desde que o prestador de serviço seja autorizado pelo fabricante, em qualquer caso, com a anuência do TJPI e com total responsabilidade da CONTRATADA, observadas as mesmas condições de habilitação e qualificação no ato convocatório.

5. Especificação técnica (art. 18, §3º, III)

5.1. Modelo de execução e gestão do contrato (art. 18, §3º, III, a)

5.1.1. Principais papéis

I – Equipe de Apoio à Contratação: equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes;

II – Equipe de Gestão da Contratação: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

III – Equipe de Fiscalização: equipe composta pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

IV – Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, sendo responsável por gerir a execução consoante às atribuições regulamentares;

V – Fiscal Demandante do Contrato: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;

VI – Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;

VII – Fiscal Técnico do contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

VIII – Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Em caso de substituição do Preposto, a CONTRATADA deverá comunicar formalmente à equipe de fiscalização, via e-mail, o nome do preposto substituto.

5.1.2. Dinâmica da Execução

5.1.2.1. Prazos e condições de entrega e recebimento do objeto

5.1.2.1.1. O prazo de entrega do objeto é de **30 (trinta) dias** consecutivos, contados a partir da publicação do extrato do Contrato ou da Ordem de Fornecimento.

5.1.2.1.1.1. Excepcionalmente, o prazo de recebimento poderá ser prorrogado por até 30 (trinta) dias, desde que solicitado pelo fornecedor e com apresentação de justificativa, nos termos do art. 57, §1º, da Lei nº 8.666/93.

5.1.2.1.1.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente que assinar o Contrato ou a Ordem de Fornecimento.

5.1.2.1.1.3. Caberá à Equipe de Fiscalização e ao setor demandante auxiliarem a autoridade competente na análise do pedido de prorrogação.

5.1.2.1.2. Por ocasião do recebimento do objeto serão aferidas a qualidade e a quantidade de acordo com

o disposto neste Termo de Referência e na proposta vencedora.

5.1.2.1.3. O objeto deverá ser entregue acompanhado da Nota Fiscal e a cópia do Contrato e/ou Ordem de Fornecimento.

5.1.2.1.4. Nos termos dos artigos 73 a 76 da lei 8.666/93, o objeto deste Termo de Referência será recebido:

a) provisoriamente, por qualquer dos membros da Equipe de Fiscalização, para efeito de posterior verificação da conformidade do material com a especificação constante neste Termo de Referência;

b) definitivamente, mediante lavratura de Termo de Recebimento Definitivo assinado pela Equipe de Gestão da Contratação, em até 10 (dez) dias úteis do término da fase de implantação, configuração e testes da solução, onde a mesma deverá estar integral e plenamente funcional no ambiente da CONTRATANTE, ocasião em que se fará constar o Atesto na Nota Fiscal.

5.1.2.1.5. Os produtos entregues em desconformidade com o especificado neste Termo ou na proposta serão rejeitados parcial ou totalmente, conforme o caso, ficando a CONTRATADA obrigada a substituí-los no prazo de até 15 (quinze) dias consecutivos, contados da data do recebimento da Notificação escrita, necessariamente acompanhada do Termo de Recusa do Material, sob pena de incorrer em atraso quanto ao prazo de execução.

5.1.2.1.5.1. A notificação de que trata o item anterior suspende os prazos de pagamento até que a irregularidade seja sanada.

5.1.2.1.6. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do material fornecido ou dos serviços prestados, cabendo-lhe sanar quaisquer irregularidades quando detectadas.

5.1.2.1.7. Comprovado que os bens e serviços entregues se enquadrem em qualquer dos casos tipificados no art. 337-L do Decreto-Lei n° 2.848/40 (Código Penal), o TJPI tomará as devidas providências, vez que é crime em prejuízo da Administração Pública, estando o autor sujeito às penas legais.

5.1.2.1.8. Na entrega do objeto, as despesas de embalagem, seguros, transportes, tributos, encargos trabalhistas e previdenciários decorrentes do fornecimento e/ou substituições do objeto, indicadas pela CONTRATANTE, deverão ser de responsabilidade da CONTRATADA, sem ônus para CONTRATANTE.

5.1.2.1.9. O produto ofertado deverá obedecer ao disposto no artigo nº. 31 da Lei Federal nº. 8.078 de 11/09/1990 (Código de Defesa do Consumidor) que diz: "A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores".

5.1.2.2. Cronograma de execução dos serviços:

5.1.2.2.1. Planejamento da implantação e entrada em operação: em até 15 (quinze) dias contados da publicação do extrato do contrato deverá ser realizada Reunião de Alinhamento entre a STIC e a CONTRATADA. Na ocasião serão acordadas as datas estimadas para entrega do objeto, implantação, testes e entrega definitiva da solução, tendo em vista os prazos acordados pelas partes.

5.1.2.2.2. Prazo de entrega da solução: a CONTRATADA deverá fornecer as licenças no prazo máximo de 30 (trinta) dias corridos contados da publicação do extrato do contrato. Excepcionalmente, o prazo retromencionado poderá ser prorrogado por mais 30 (trinta) dias desde que solicitado pela CONTRATADA acompanhado de justificativa e aprovação por parte da Administração.

5.1.2.2.3. Fase de implantação, configuração e testes da solução: a CONTRATADA deverá realizar a implantação, configuração e testes com base nas diretrizes e comandos apontados pelo gerente do projeto da CONTRATANTE, neste Termo de Referência e no acordado no item 5.1.2.2.1. Nesse período, a solução passará por testes extensivos realizados pela equipe da CONTRATANTE. A aprovação desta fase pelo gerente do projeto da CONTRATANTE configura condição necessária para a expedição do termo de recebimento definitivo ou documento equivalente.

5.1.2.2.4. Prazo para emissão do Termo de Recebimento Definitivo ou documento equivalente: em até 10 (dez) dias úteis do término da fase de implantação, configuração e testes da solução a equipe de planejamento da contratação fornecerá o Termo de Recebimento Definitivo atestando a regularidade do fornecimento e dando início ao prazo da garantia da solução.

5.1.2.2.4.1. A emissão do Termo de Recebimento Definitivo está condicionada à entrega do documento atestando o início e o fim da vigência da garantia da solução contratada englobando todos os seus itens e serviços contratados (doravante nomeado de "CERTIFICADO DE GARANTIA") para verificação por parte da equipe de fiscalização.

5.1.2.2.4.2. Para fins de recebimento do Item 3 – Serviço de implantação – poderá ser aceita a diferença entre a quantidade de licenças adquiridas e efetivamente utilizadas, desde que decorra diretamente de fato da Administração e que o lote residual das licenças seja disponibilizado para que o setor técnico promova oportunamente a implantação com suporte e orientação da Contratada durante todo o período de vigência;

5.1.2.2.5. Cronograma da realização dos treinamentos: Caso haja, preferencialmente os treinamentos serão realizados antes da fase especificada do item 5.1.2.2.1. deste Termo, de acordo com o cronograma pactuado na Reunião de Alinhamento. Alternativamente, poderá ser definido prazo distinto deste item, como por exemplo, seguir o calendário oficial de treinamentos do fabricante do software da solução, desde que acordado expressamente entre CONTRATANTE e CONTRATADA.

5.1.2.3. Instrumentos formais de solicitação de fornecimento:

5.1.2.3.1. Documento de solicitação de fornecimento: Contrato ou Ordem de fornecimento devidamente assinado por ambos os contratantes.

5.1.2.3.2. Documento de recebimento provisório: Termo de Recebimento Provisório assinado pela Equipe de Fiscalização da contratação.

5.1.2.3.3. Documento de recebimento definitivo: Termo de Recebimento Definitivo assinado pela Equipe de Gestão da contratação.

5.1.2.3.4. Solicitações de chamado técnico:

a) Chamado Técnico por meio de Mensagem eletrônica (e-mail) como ferramenta preferencial de solicitação, acompanhamento e de aferição do serviço prestado pela CONTRATADA;

b) Chamado Técnico de forma eletrônica por meio de Central on-line;

c) Chamado Técnico por meio telefônico para a Central de Atendimento.

5.1.2.4. Prazos de garantia, suporte e Níveis Mínimos de Serviço Exigidos (NMSE)

5.1.2.4.1. Período de garantia técnica: 12 (doze) meses, contados a partir do recebimento definitivo do objeto.

5.1.2.4.2. Durante o prazo de garantia técnica, a CONTRATADA deverá garantir o funcionamento da solução como um todo, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção, incluindo:

5.1.2.4.2.1. Atualizações corretivas e evolutivas, de *drivers*, *firmwares*, *softwares* e manuais, durante

a vigência da garantia e suporte da solução;

5.1.2.4.2.2. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

5.1.2.4.2.3. Demais procedimentos destinados a recolocar a solução em perfeito estado de funcionamento;

5.1.2.4.2.4. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

5.1.2.4.2.5. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização, *troubleshooting* ou utilização dos produtos adquiridos.

5.1.2.4.3. A CONTRATADA deverá apresentar, até a data do recebimento definitivo da implantação, instrumento que comprove, junto ao fabricante, o início do serviço de suporte técnico da solução.

5.1.2.4.4. A garantia deverá incluir todas as atualizações de todos os softwares que compõem a solução durante o período contratado.

5.1.2.4.5. Devem ser disponibilizados serviços de suporte durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que acionados pela CONTRATANTE, mediante a abertura de chamado técnico, prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional;

5.1.2.4.6. Os serviços de atendimento da Central de Assistência técnica deverão ser providos das seguintes formas:

5.1.2.4.6.1. Um canal de suporte técnico através de um número telefônico de serviço, em língua portuguesa, para abertura de chamados técnicos de hardware e software. Este serviço deverá obrigatoriamente estar disponível 8x5 (oito horas por dia, 5 dias por semana, durante o horário comercial) sem custos para a CONTRATANTE;

5.1.2.4.6.2. Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado de forma ininterrupta 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.1.2.4.6.3. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso (somente leitura) para acompanhamento de chamados de suporte e manutenção abertos;

5.1.2.4.6.4. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso para consulta de documentação técnica do fabricante e atualizações de software;

5.1.2.4.7. Os chamados técnicos deverão possuir identificador de ocorrência próprio, data e hora de abertura devidamente repassada a CONTRATANTE, a fim de registro e acompanhamento das ocorrências;

5.1.2.4.8. A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento das ocorrências e de seus estados;

5.1.2.4.9. Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações:

A) Número do chamado;

B) Categoria de prioridade;

C) Descrição do problema e da solução;

D) Procedimentos realizados (passo a passo);

E) Data e hora da abertura e do fechamento do chamado;

F) Data e hora do início e do término da execução dos serviços; e

G) Identificação do técnico da empresa.

5.1.2.4.10. O tempo de solução para os chamados técnicos abertos será contado a partir do registro dos mesmos em qualquer um dos meios disponíveis da Central de Atendimento da CONTRATADA;

5.1.2.4.10.1. O encerramento do chamado será dado por técnico da CONTRATANTE na conclusão dos serviços;

5.1.2.4.11. Em caso de atraso na conclusão do atendimento, em qualquer nível de prioridade, será admitida a proposição, pela CONTRATADA, de justificativa técnica, a qual deverá conter os motivos do atraso, acompanhados da devida comprovação;

5.1.2.4.11.1. A justificativa eventualmente apresentada será analisada pela Administração a qual emitirá parecer, para fins de sua aceitação ou não;

5.1.2.4.11.2. Em sendo aceita, ocorrerá tão somente a interrupção dos prazos contratuais, sem prejuízo da conclusão do chamado. Em não sendo aceita, impor-se-á as sanções previstas neste documento, bem como no Termo de Referência e eventual Contrato Administrativo.

5.1.2.4.11.3. Não será aceita justificativa cujo teor funde-se na:

a) Falta de mão de obra disponível para atendimento dentro dos prazos contido nos Níveis Mínimos de Serviços Exigidos (NMSE);

5.1.2.4.11.4. A justificativa deverá ser apresentada em até 03 (três) dias úteis da conclusão do chamado. Uma vez apresentada fora deste prazo, caberá à Administração conhecer ou não o documento;

5.1.2.4.12. A CONTRATADA/FABRICANTE devera disponibilizar site na internet incluindo pelo menos a relação de licenças de uso disponíveis, base de conhecimento, fórum de discussão, documentação técnica dos produtos ofertados, comunidades técnicas, abertura e acompanhamento do histórico de chamados, sem limite de quantidade, download de produtos, atualizações e correções;

5.1.2.4.13. Durante todo período de vigência do contrato de suporte o Tribunal de Justiça do Estado do Piauí terá direito a atualização de versão de Software para todas as licenças de uso;

5.1.2.4.14. Os **Níveis Mínimos de Serviços Exigidos (NMSE)** serão classificados conforme os níveis de severidade a seguir:

Nível de Severidade	Descrição	Prazo de Atendimento	Prazo de Solução Definitiva
ALTA	Esse nível de severidade é aplicado quando há indisponibilidade de qualquer item (componente da solução) apresentando falha de funcionamento ou impactando diretamente toda a infraestrutura da solução;	02 (duas) horas	24 (vinte e quatro) horas
MÉDIA	Esse nível de severidade é aplicado quando há falha, simultânea ou não, de qualquer item (componente da solução) que não inviabilize o uso da solução, mas diminua alguma funcionalidade ou afete negativamente a performance;	04 (quarto) horas	48 (quarenta e oito) horas
	Este nível de severidade é aplicado para instalação, configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento de todos os software(s) componentes da solução. Ou seja,		

BAIXA	chamados técnicos que não requeiram imediato atendimento e/ou solução. Para efeitos de Acordo de Nível de Serviço (SLA), não haverá abertura de chamados técnicos com esta severidade em sábados, domingos e feriados, sendo o tempo de SLA deslocado para o seguinte dia útil, horário comercial.	06 (seis) horas	72 (setenta e duas) horas

5.1.2.4.15. Os Níveis Mínimos de Serviços Exigidos (NMSE) serão tratados da seguinte forma:

a. Prazo de Solução Definitiva: Tempo decorrido entre a abertura de chamado técnico efetuada pelo Fiscal Técnico ou Gestor do Contrato e a efetiva recolocação da solução em seu pleno estado de funcionamento;

b. Caso seja verificado que a solução apresentada pela empresa não resolveu o problema definitivamente, o chamado será reaberto pelo Fiscal Técnico ou Gestor do Contrato retomando-se a contagem do prazo de solução definitiva a partir do momento de sua interrupção.

c. O atendimento aos chamados técnicos de criticidade ALTA poderá ser realizado também de forma on-site, desde que solicitado pelo Fiscal Técnico ou Gestor do Contrato;

d. A interrupção do suporte de um chamado técnico classificado no tipo de criticidade MÉDIA ou ALTA pela CONTRATADA e que não tenha sido previamente autorizado pelo Fiscal Técnico ou Gestor do Contrato, poderá ensejar em aplicação de penalidades previstas.

e. Após a conclusão do serviço de suporte, a equipe técnica da CONTRATADA comunicará formalmente (preferencialmente por mensagem eletrônica) ao Fiscal Técnico ou Gestor do Contrato e solicitará autorização para o fechamento do chamado;

f. Entende-se por término do atendimento técnico a hora em que a solução for disponibilizada para uso em perfeitas condições de funcionamento, estando condicionado à aprovação da CONTRATANTE.

g. Caso não seja confirmada a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, o Fiscal Técnico ou Gestor do Contrato informará as pendências relativas ao chamado aberto.

h. Em casos excepcionais, o Fiscal Técnico ou Gestor do Contrato poderá solicitar o escalonamento de chamado para níveis superiores de criticidade. Nesse caso, o escalonamento deverá ser justificado e os prazos dos chamados técnicos reiniciar-se-ão.

i. Sempre que houver quebra dos níveis de serviços exigidos ou problemas que afetem a execução do objeto, o Gestor do Contrato enviará notificação por mensagem eletrônica para a CONTRATADA que terá o prazo de até 48 (quarenta e oito) horas corridas e contadas a partir do recebimento da notificação para apresentar as justificativas para as falhas verificadas;

j. Caso não haja manifestação no prazo constante no item anterior ou caso o Gestor do Contrato entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

5.1.2.5. GARANTIA E ATUALIZAÇÃO DOS SOFTWARES

5.1.2.5.1. Todos os softwares deverão ter suporte técnico e atualização de versões, enquanto a assinatura do serviço estiver ativa.

5.1.2.5.2. No caso de bugs ou falhas no software, a empresa CONTRATADA deverá fornecer atualizações necessárias à correção do problema, independentemente de tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA;

5.1.2.5.3. A cada nova liberação de versão, a CONTRATADA deverá fornecer as atualizações de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas;

5.1.2.5.4. As novas versões dos produtos contratados, quando aplicável, deverão ser disponibilizadas imediatamente, a partir do lançamento oficial da nova versão;

5.1.2.5.5. Será permitido à CONTRATADA entregar os todos os documentos e manuais técnicos relativos a solução por meio eletrônico.

5.1.2.6. Mecanismos formais de comunicação:

5.1.2.6.1. Toda a comunicação entre a CONTRATADA e a CONTRATANTE será realizada, preferencialmente, por mensagem eletrônica (e-mail) ou por sistema de abertura e acompanhamento de chamados (help desk) com registro de data/hora.

5.1.2.6.2. Excepcionalmente e em casos de urgência ou iminência de parada total da solução, o TJPI poderá realizar solicitações verbais à CONTRATADA. Entretanto, nesses casos, todas as ações tomadas pela CONTRATADA deverão ser reduzidas a termo para posterior validação por parte do Fiscal Técnico ou Gestor do Contrato.

5.1.2.6.3. Além da reunião de alinhamento e validação de expectativas, deverão ser realizadas, se necessárias, outras reuniões presenciais ou não entre o Gestor do Contrato e o Preposto da CONTRATADA para avaliação do(s) serviço(s) prestado(s) no período, e verificação do atendimento aos requisitos contratuais estabelecidos;

5.1.2.6.4. Poderão ser realizados, alternativamente, e a critério do Gestor do Contrato, o controle e o acompanhamento da prestação de serviço mediante o uso de mensagens eletrônicas. Nesse caso, o Fiscal Técnico ou Gestor do Contrato deverá apresentar descritivo contendo situações merecedoras de avaliação por parte da CONTRATADA.

5.1.2.7. Transferência de conhecimento:

5.1.2.7.1. Os seguintes procedimentos deverão ser seguidos durante toda a execução do objeto, em especial durante a prestação de serviço de garantia técnica:

i. A equipe da CONTRATADA deverá apresentar ao Fiscal Técnico do Contrato de forma objetiva e por escrito todos os procedimentos realizados nos chamados abertos pelo TJPI em vistas de problemas ou interrupções na solução que forem sanados.

ii. Para que ocorra a transferência de conhecimento, no fechamento dos chamados técnicos de garantia técnica, a CONTRATADA deverá apresentar por mensagem eletrônica ou em documento apropriado, a solução para o problema que originou a abertura do chamado;

iii. O envio da solução pelos meios devidos não exime a Contratada da apresentação do Relatório Gerencial de Serviços com a consolidação dos chamados técnicos abertos;

iv. Os conhecimentos técnicos repassados para a equipe da Secretaria de Tecnologia da Informação serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do TJPI não sejam prejudicadas ou interrompidas.

5.1.2.8. Direitos de propriedade intelectual, sigilo e restrições

5.1.2.8.1. Os direitos de propriedade intelectual permanecerão de posse da empresa fabricante do produto a ser adquirido, não havendo transferência de direitos de propriedade em face de contratação, salvo os direitos de uso da solução contratada.

5.1.2.9. Qualificação técnica e formação dos profissionais envolvidos

5.1.2.9.1. Os profissionais da CONTRATADA deverão possuir qualificação condizente com o fornecimento do objeto. Em especial, deverão possuir certificação ou declaração emitida pela fabricante da solução a ser fornecida que ateste sua qualificação técnica na operação, manutenção e implementação da mesma.

5.1.2.9.2. Caso o profissional que irá realizar a implantação da solução seja subcontratado, este profissional deverá possuir certificação ou declaração emitida pela fabricante da solução a ser fornecida que ateste sua qualificação técnica na operação, manutenção e implantação da mesma.

6. REQUISITOS TÉCNICOS ESPECÍFICOS (art. 18, §3º, IV)

ITEM 1

6.1. SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (XDR)

6.1.1. Aquisição de licenças de solução de segurança para proteção avançada de endpoints (estação de trabalho e servidores) no combate a vírus, malwares conhecidos e desconhecidos, vulnerabilidades conhecidas e desconhecidas com características estendidas de detecção e resposta;

6.1.2. As funcionalidades de proteção que compõe a solução de segurança, podem funcionar em múltiplos equipamentos e/ou softwares desde que obedeçam a todos os requisitos desta especificação;

6.1.3. A solução deve possuir a capacidade e vir licenciada para integrar-se com a solução de firewall do fabricante Palo Alto Networks, implantada no órgão, permitindo utilizá-la como parte da solução de segurança suportando o monitoramento do tráfego de rede e correlacionando os eventos de segurança da camada de rede com os eventos ocorridos nos endpoints protegidos de modo centralizado, proporcionando uma análise de risco mais assertiva e completa;

6.1.4. Deverão estar inclusas na proposta todas as licenças necessárias para o pleno funcionamento da solução, conforme as especificações elencadas;

6.1.5. A solução deve vir licenciada para retenção de logs pelo período mínimo de 30 dias, o que deve incluir o cluster de Firewall da Palo Alto Networks, modelo PA-5220, composto por 2 appliances, além dos logs dos agentes de proteção de endpoint, inerentes à solução.

6.1.5.1. A solução deve permitir a expansão desse período de retenção de logs, conforme as necessidades da instituição, devendo ser licenciado posteriormente, conforme o caso.

6.1.6. A solução deve possuir subscrição pelo período mínimo de 12 (doze) meses, permitindo, durante este período, acesso ilimitado à console central de gerenciamento na nuvem, acesso a todas as atualizações, serviços de segurança e assinaturas de proteção da solução e o pleno funcionamento do agente de proteção instalado nos endpoints.

6.2. CARACTERÍSTICAS GERAIS

6.2.1. Entende-se por Endpoint uma estação de trabalho, servidor de rede ou dispositivo móvel;

6.2.2. A proteção avançada dos endpoints deve ser feita através da instalação de agentes nos endpoints, devendo suportar, pelo menos os seguintes sistemas operacionais:

6.2.2.1. Android 6 e superiores;

6.2.2.2. Windows Vista;

6.2.2.3. Windows 7;

6.2.2.4. Windows 8;

6.2.2.5. Windows 8.1;

6.2.2.6. Windows 10;

6.2.2.7. Mac OS X 10.13 e superiores;

6.2.2.8. Windows Server 2003;

6.2.2.9. Windows Server 2003 R2;

6.2.2.10. Windows Server 2008;

6.2.2.11. Windows Server 2008 R2;

6.2.2.12. Windows Server 2012;

6.2.2.13. Windows Server 2012 R2;

6.2.2.14. Windows Server 2016;

6.2.2.15. Windows Server 2019

6.2.2.16. Windows Server Datacenter

6.2.2.17. RHEL/CentOS/Oracle Linux 6 e superiores;

6.2.2.18. Debian Linux 9 e superiores;

6.2.2.19. Ubuntu Linux 12 e superiores;

6.2.3. Deve suportar e possuir agente para máquinas virtuais instaladas em ambiente VMware;

6.2.4. Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução;

6.2.5. Proteção contra a desativação não autorizada dos serviços que compõem a solução;

6.2.6. Ser eficaz na prevenção de vulnerabilidades e malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem;

6.2.7. O agente de endpoint deve continuar funcionando e aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado;

6.2.8. Impedir executável malicioso, sem requerer nenhum conhecimento prévio do artefato;

6.2.9. Deve prevenir contra ameaças conhecidas baseado em assinatura;

6.2.10. Deve prevenir contra ameaças baseada em comportamento através do monitoramento das atividades realizadas pelo endpoint;

6.2.11. Deve prevenir contra ameaças através do uso de machine learning através da análise local de arquivos desconhecidos;

6.2.12. Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real;

6.2.13. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados;

6.2.14. A solução deve permitir implementação em modo de monitoramento ou aprendizado do ambiente em fase inicial de instalação;

6.2.15. A solução deve fornecer a capacidade de configurar listas brancas globais para permitir que

determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição;

6.2.16. A solução deve ter a capacidade de criar, a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint;

6.2.17. Deve permitir bloquear nos endpoints o uso de dispositivos portáteis USB como pen drives, discos, drives de CD/DVD/BluRay a fim de prevenir contra a transferência de arquivos maliciosos por meio destes dispositivos;

6.2.18. Deve possuir firewall de host permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego;

6.2.19. A solução deve armazenar as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período mínimo de 30 (trinta) dias;

6.3. PROTEÇÃO CONTRA VULNERABILIDADES

6.3.1. A solução deve suportar a proteção de processos e aplicativos em execução no sistema operacional;

6.3.2. A solução deve suportar a adição de aplicações proprietárias e personalizadas na lista de aplicações protegidas;

6.3.3. A solução deve ser capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória e sequestro de DLL;

6.3.4. A solução deve ser capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração;

6.3.5. Ao impedir ou bloquear uma técnica de exploração, a solução deve congelar o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo;

6.3.6. Ao impedir ou bloquear uma técnica de exploração, a solução deve finalizar apenas o processo específico alvo do ataque;

6.3.7. A solução deve utilizar módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração devem proteger aplicações conhecidas, bem como aplicações desconhecidas e desenvolvidas internamente pela instituição;

6.3.8. A solução deve ser capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança da console de gerenciamento da solução;

6.3.9. Suportar detecção e bloqueio de, no mínimo, os seguintes métodos, devendo ser capaz de:

6.3.9.1. Impedir execução de dados na memória;

6.3.9.2. Impedir acessos não autorizados a DLLs do sistema;

6.3.9.3. Prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos;

6.3.9.4. Interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado;

6.3.9.5. Prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração em processadores de texto;

6.3.9.6. Prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memoria. Exemplo: “free() double”;

6.3.9.7. Prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória);

6.3.9.8. Obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração;

6.3.9.9. Ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade;

6.3.9.10. Prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc;

6.3.9.11. Proteger o acesso a metadados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória;

6.3.9.12. Agir preventivamente contra heap spray ao checar periodicamente a zona heap da memória virtual;

6.3.9.13. Prevenir a exploração de vulnerabilidade através da pré-alocação aleatória do layout de memória de processos no sistema operacional;

6.3.9.14. Prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações “Just-in-time” (JIT);

6.3.9.15. Mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, impedindo a execução de código malicioso arbitrário no sistema operacional;

6.3.9.16. Reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo;

6.3.9.17. Prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória;

6.3.9.18. Prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0);

6.3.9.19. Aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR;

6.4. PROTEÇÃO CONTRA MALWARE

6.4.1. A solução deve suportar a proteção contra a execução de arquivos maliciosos;

6.4.2. A solução deve fornecer a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem executar incluindo proteção contra criação de processos filhos;

6.4.3. A solução deve ser capaz de fornecer prevenção contra malware desconhecido usando análise dinâmica em ambiente de sandbox;

6.4.4. A solução deve possuir integração com o serviço de análise de malwares desconhecidos em nuvem (sandbox) para uma análise mais profunda dos arquivos;

6.4.4.1. Deve fornecer veredito e relatório informando o resultado da análise em sandbox;

6.4.5. O serviço de análise em nuvem pode ser do mesmo fabricante da solução de proteção avançada de endpoint ou de fabricantes terceiros devendo ser fornecidas todas as licenças necessárias para seu pleno funcionamento;

6.4.6. O serviço de análise de malwares desconhecidos em nuvem deve possuir a capacidade de realizar a análise dos arquivos em ambientes bare metal para detectar malwares VM-aware, que possuem a capacidade de detectar que estão em um ambiente virtual e nesta situação não realizam as atividades maliciosas para as quais foi desenvolvido;

6.4.7. O serviço de análise de malwares desconhecidos em nuvem deve realizar a análise de, no mínimo, os seguintes tipos de arquivos: arquivos executáveis, DLLs, arquivos Word (.doc, .docm e docx) e Excel (.xls, .xlsm e .xlsx) que contenham macros, arquivos DMG e arquivos ELF;

6.4.8. A solução deve fornecer a capacidade de criar exceções para hash específicos de arquivos analisados em nuvem na solução de sandbox;

6.4.9. A solução deve fornecer a capacidade de impedir a execução de um arquivo quando seu valor de hash for desconhecido pela solução de sandbox;

6.4.10. A solução deve fornecer a capacidade de impedir a execução de um arquivo quando o hash do arquivo for desconhecido por cache local e o mesmo não tiver comunicação com o servidor de gerência;

6.4.11. Deve permitir executar a varredura no endpoint em busca de arquivos infectados por malware a partir da console central de gerenciamento e a partir do próprio agente instalado no endpoint. Deve ser possível também configurar varreduras agendadas;

6.4.12. Caso um malware seja detectado, deve ser possível o envio do mesmo para quarentena automaticamente através de política pré-definida na gerência centralizada;

6.4.13. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo e não apenas por sua extensão;

6.4.14. Deve extrair o hash de arquivos executáveis e verificar se o mesmo já foi analisado na solução de sandbox de forma automática sem necessidade de scripts externos ou adaptações não nativas da solução. Caso o malware já tenha apresentado comportamento malicioso em sandbox, o mesmo deve ser impedido de ser executado no endpoint;

6.4.15. Deve possuir mecanismos para detectar, em tempo real, ataques LotL – Living off the Land, ataques baseados em scripts e ataques fileless (sem arquivos);

6.4.16. Deve permitir ao administrador reportar falsos positivos na análise de malwares em sandbox. A solução deve informar ao administrador o resultado desta análise e exibir a correção na gerência da solução;

6.4.17. Deve avisar o usuário quando a execução de um arquivo for bloqueada incluindo casos quando não houver veredito da sandbox sobre o arquivo e o seu status estiver definido como desconhecido;

6.4.18. Deve possibilitar o bloqueio automático de malwares já descobertos através da sandbox do fabricante em outros endpoints do órgão;

6.4.19. Deve ser capaz de restringir a execução de arquivos específicos somente em diretórios conhecidos e protegidos, tanto na maquina local quanto em drives remotos;

6.4.20. Deve prevenir execução de arquivos não assinados;

6.4.21. Deve prevenir a execução de arquivos em mídia externa;

6.4.22. Deve ser capaz de controlar executáveis não assinados por meio do uso de WhiteLists;

6.4.23. Deve ser capaz de restringir a execução de processos;

6.4.24. Deve possuir a capacidade de controlar e limitar a criação de processos filhos;

6.4.25. Deve possibilitar o controle de arquivos conhecidos e não conhecidos;

6.4.26. Deve ser capaz de definir e classificar Hashs conhecidos.

6.5. COLETA DE INFORMAÇÕES FORENSES

6.5.1. A solução deve coletar dados forenses capturados pelo agente de endpoint, contemplando, pelo menos, os seguintes:

6.5.1.1. Dump de memória;

6.5.1.2. Arquivos Acessados;

6.5.1.3. Módulos carregados;

6.5.1.4. URIs acessadas;

6.5.1.5. Local de execução do arquivo;

6.5.1.6. Tempo de execução;

6.5.1.7. Nome do arquivo;

6.5.1.8. Hash do arquivo;

6.5.1.9. Nome do usuário relacionado;

6.6.. Nome do computador;

6.5.1.11. Endereço IP;

6.5.1.12. Versão de sistema operacional;

6.5.1.13. Histórico de arquivos maliciosos;

6.6. GERENCIAMENTO

6.6.1. A console de gerenciamento deverá ser baseada em nuvem e acessada através de navegadores web, devendo conter de forma centralizada os recursos para a monitoração e controle da proteção dos dispositivos;

6.6.2. A console deverá apresentar Dashboard com o resumo do estado de proteção dos dispositivos protegidos, bem como indicar os alertas de eventos de criticidades alta, média e baixa;

6.6.3. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

6.6.4. A console deve permitir, dentro da estrutura de gerenciamento, a organização dos dispositivos protegidos em grupos;

6.6.5. Deve permitir a aplicação de regras diferenciadas baseadas em dispositivos ou grupos de dispositivos;

6.6.6. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

6.6.7. A solução deverá ser compatível, no mínimo, com os navegadores (web browsers) Firefox e

Chrome;

6.6.8. Caso a solução necessite de Banco de Dados (Ex. SQL Server Enterprise), deverão estar inclusas na proposta as licenças necessárias para seu pleno funcionamento;

6.6.9. A comunicação entre a console de gerenciamento e os clientes gerenciados deve ser feita através do uso de protocolos seguros e protegidos por criptografia;

6.6.10. Deve ser possível realizar acesso direto aos endpoints protegidos a partir da console central de gerenciamento da solução, a fim de permitir a execução de ações para investigação e reposta aos incidentes de segurança como: visualizar e encerrar processos, apagar, mover e renomear arquivos, prover interface de linha de comando capaz de executar comandos do sistema operacional e executar scripts e comandos python nos endpoints;

6.6.11. Deve ser possível salvar um relatório contendo todas as atividades realizadas durante a sessão de acesso aos endpoints gerenciados;

6.6.12. Deve ser possível realizar, a partir da console de gerenciamento, a execução simultânea de scripts nos diversos endpoints de forma centralizada;

6.6.13. A solução deve permitir, a partir da console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede;

6.6.14. Deve possuir mecanismo de comunicação pré-definido, em tempo determinado e configurável pelo administrador, entre os agentes nos endpoints e a console de gerenciamento, provendo a consulta de novas configurações, políticas ou conteúdo;

6.6.15. Permitir a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução;

6.6.16. Deve registrar nos logs as alterações realizadas pelos administradores da solução, provendo auditoria de mudanças;

6.6.17. A solução deve ser capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs;

6.6.18. A atualização do motor de detecção de ameaças deve ser realizada de forma transparente para o usuário;

6.6.19. Deve permitir integração com soluções de SIEM enviando logs no formato Syslog ou compatível;

6.6.20. Deve se comunicar, por meio de logs de incidentes e ataques ou informações de inteligência, com os elementos de segurança do ambiente, como por exemplo, mas não se limitando a: Firewalls, Proxies, Filtros de Conteúdo;

6.6.21. Deve exibir lista com todos os alertas de incidentes detectados na console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP envolvido, a ação tomada pelo agente com relação ao incidente e a categoria do incidente informando se o mesmo se trata de exploit ou malware, por exemplo;

6.6.22. Deve permitir notificar eventos ao administrador por e-mail;

6.6.23. Deve permitir a criação de políticas para prevenção e mitigação de:

6.6.23.1. Vulnerabilidades conhecidas e desconhecidas (Exploits);

6.6.23.2. Códigos Maliciosos (Malware);

6.6.23.3. Restrições de execução;

6.6.24. Deve centralizar e gerenciar na console de administração qualquer evento de segurança detectado, seja na camada de rede ou nos endpoints protegidos;

6.6.25. Deve ser exibida também, na console central de gerenciamento, a lista de CVE – Common Vulnerabilities and Exposures – conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE;

6.6.26. Deve identificar e gerar log de qualquer interferência no serviço de proteção nas estações e servidores protegidos, como por exemplo:

6.6.26.1. Tentativa de encerramento do processo de proteção;

6.6.26.2. Tentativa de encerramento do serviço de proteção;

6.6.26.3. Logs de sistema relacionados a tentativa de interferência com o serviço, processo ou arquivos do sistema de proteção;

6.6.27. Deve ser possível visualizar, em uma linha do tempo, a cadeia de processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Para cada processo executado deve ser possível visualizar, no mínimo, o caminho onde o processo estava localizado, o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo;

6.6.28. Além dos processos executados deverão ser exibidas informações sobre conexões de entrada e saída, conexões fracassadas e download e upload de dados;

6.6.29. A solução deve permitir o ajuste de políticas de coleta de informações forenses, dentro da console de gerenciamento centralizado, com definições do tipo de informações sobre o incidente que serão coletadas quando uma ameaça ou ataque for identificado;

6.6.30. Deve possuir ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e do Linux. Deve permitir também realizar a busca através da combinação destes atributos;

6.6.31. Deve ser possível a realização de busca com base no caminho completo onde o arquivo pode estar localizado e também com base no hash do arquivo gerado pela solução.

6.6.32. A solução deve permitir realizar a configuração de alertas com base em incidentes e em indicadores de comprometimento, como nome do arquivo, domínio e endereço IP de destino. A solução deve permitir importar listas de indicadores de comprometimento de serviços externos de inteligência contra ameaça, além de permitir a criação destes indicadores;

6.6.33. A solução deve permitir realizar a configuração de alertas baseados no comportamento do endpoint. Os tipos de comportamentos que devem ser detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede, escalonamento de privilégio e movimentos laterais na rede;

6.6.34. A solução deve permitir realizar a atualização de versão dos agentes instalados nos endpoints a partir da console central de gerenciamento;

6.6.35. A solução deve receber e distribuir atualizações contendo ajustes finos de políticas de proteção, de módulos de proteção e novos modelos matemáticos para uso de aprendizagem de máquina (Machine Learning) para análise de código antes da execução;

6.7. RELATÓRIOS

6.7.1. A solução deve fornecer visualização das ameaças em formato Web;

6.7.2. A solução deve suportar exportação no formato CSV dos eventos relacionados à ameaças, bem como o status dos agentes de endpoints;

6.7.3. Capacidade de geração de relatórios, estatísticas e gráficos contendo no mínimo os seguintes tipos pré-definidos:

6.7.3.1. As 10 máquinas com maior ocorrência de códigos maliciosos;

6.7.3.2. Os 10 usuários com maior ocorrência de códigos maliciosos;

6.7.3.3. Localização dos códigos maliciosos;

6.7.3.4. Sumário das ações realizadas;

6.7.3.5. Número de infecções detectadas diária, semanal e mensalmente;

6.7.4. Deve abranger os códigos maliciosos detectados;

6.7.5. A solução deverá ter os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição:

6.7.5.1. Relatório de restrição de acesso a arquivos e processos;

6.7.5.2. Técnicas de Malwares utilizadas;

6.7.5.3. Técnicas de exploração utilizadas;

6.7.5.4. Informações Forenses coletadas.

6.7.6. A solução deverá ter os seguintes dashboards de controle para monitorar a situação dos endpoints da instituição:

6.7.6.1. Detalhes da saúde dos agentes de endpoints;

6.7.6.2. Dashboard de controle do histórico de regras dos endpoints;

6.7.6.3. Dashboard de controle da Política de Segurança instalada nos endpoints;

6.7.6.4. Dashboard de controle do histórico de status do serviço nos endpoints;

ITEM 2

6.8. GERENCIAMENTO DE VULNERABILIDADES E INVENTÁRIO

6.8.1. Deve prover informações capazes de enriquecer a análise de segurança do ambiente, aumentando a visibilidade e fornecendo melhor compreensão dos riscos;

6.8.2. Deve prover elementos capazes de neutralizar rapidamente ameaças à segurança institucional;

6.8.3. Deve reduzir os esforço do diagnóstico ao fornecer informações abrangentes e suficientes permitindo melhorar o tempo de resposta dos incidentes;

6.8.4. Deve prover, de forma rápida e simples, recurso capaz de realizar a busca e a remoção do arquivo malicioso de todos os endpoints gerenciados;

6.8.5. Deve possuir o recurso de inventário, sendo capaz de exibir, em detalhes, diversas informações dos sistemas dos endpoints;

6.8.6. Deve exibir detalhes sobre os aplicativos instalados que requerem e receberam permissões especiais para habilitar uma câmera, microfone, recursos de acessibilidade, acesso total ao disco ou capturas de tela;

6.8.7. Deve exibir detalhes sobre executáveis que iniciam automaticamente quando o usuário efetua login ou inicializa o sistema operacional do dispositivo protegido;

6.8.8. A solução deve exibir informações sobre autoruns que são configurados no registro do endpoint, pastas de inicialização, tarefas agendadas, serviços, drivers, daemons, extensões, tarefas Crond, itens de login, ganchos de login e logout;

6.8.9. Para cada execução automática, a solução deve listar o tipo e a configuração da execução automática, como método de inicialização, CMD, detalhes do usuário e caminho da imagem;

6.8.10. Deve exibir, pelo menos os seguintes detalhes, para cada daemon existente no endpoint gerenciado:

6.8.10.1. Nome, tipo, caminho e estado, indicando se está carregado, em execução ou não;

6.8.11. Deve exibir detalhes sobre cada volume de disco existentes em um endpoint, como os seguintes:

6.8.11.1. Tipo de unidade, nome, sistema de arquivos, espaço livre e tamanho total;

6.8.11.2. Deve mostrar informações como nome, tipo, caminho, modo e estado de todos os drivers instalados em um dispositivo gerenciado;

6.8.12. Deve exibir detalhes sobre todas as unidades, volumes e discos que foram montados no endpoint, a exemplo das seguintes:

6.8.12.1. Listar o diretório do ponto de montagem, o tipo de sistema de arquivos, especificações da montagem e GUID;

6.8.13. Deve detalhar, para cada serviço em execução em um endpoint, informações como:

6.8.13.1. Nome, tipo, caminho, status do tempo de execução, se o serviço está em execução e qual é o estado do tempo de execução, se o serviço pode ser parado, pausado ou atrasado seu horário de início, se o serviço requer interação com a área de trabalho do endpoint, o nome do usuário que iniciou o serviço e o modo de início

6.8.14. Deve mostrar detalhes sobre cada pasta compartilhada em rede como:

6.8.14.1. Tipo de pasta de rede compartilhada: Disk Drive, Print Queue, Device, IPC, Disk Drive Admin, Print Queue Admin, Device Admin, IPC Admin;

6.8.14.2. Nome da pasta, descrição e caminho;

6.8.14.3. Se a pasta está limitada a um número máximo de compartilhamentos e o número máximo de compartilhamentos permitidos;

6.8.15. Deve apresentar informações gerais sobre o hardware do endpoint, como fabricante, modelo, memória física, arquitetura de processadores e CPU;

6.8.16. Deve apresentar informações sobre o sistema operacional e a release em execução no endpoint;

6.8.17. A solução deve fornecer a lista de usuários cujas credenciais estão armazenadas no endpoint;

6.8.18. Deve fornecer informações sobre as contas de usuários, quais estão ativas e o tipos de cada uma;

6.8.19. Deve informar detalhes sobre a senha definida para cada conta de usuário, como se ela é necessária para fazer login, se tem uma data de validade ou se pode ser alterada;

6.8.20. Deve mostrar informações de conexões dos ativos em forma de gráficos a fim de simplificar a investigação e proporcionar ganho de eficiência.

6.8.21. Deve ser capaz de identificar e quantificar as vulnerabilidades de segurança (CVEs) existentes para as aplicações instaladas nos endpoints;

6.8.22. Deve oferecer visibilidade em tempo real da exposição às vulnerabilidades e dos níveis de patch atuais dos endpoints, aperfeiçoando a análise de gravidade dos riscos e permitindo priorizar a mitigação.

6.8.23. Deve ser uma solução eficaz no gerenciamento de vulnerabilidade, devendo ser simples de utilizar, escalonável e do mesmo fabricante da solução avançada de proteção de endpoint.

ITEM 3

6.9. SERVIÇO DE IMPLANTAÇÃO

6.9.1. Características Gerais do Serviço de Implantação e Configuração da Solução de Endpoint.

6.9.1.1. Os serviços deverão ser executados pela CONTRATADA, por técnicos comprovadamente credenciados pelo fabricante;

6.9.1.2. A CONTRATADA deverá informar nome, e-mail e telefone dos componentes da equipe técnica responsável pela solução, ou seja, do gerente do projeto, técnico e do responsável comercial;

6.9.1.3. Após o recebimento do Pedido de Compra, a CONTRATADA tem o prazo máximo de 15 (quinze) dias para realizar a Reunião de Alinhamento do Projeto, que deverá ser feita de forma remota, onde a CONTRATADA deverá apresentar os técnicos responsáveis pela implantação e suas respectivas documentações exigidas neste Termo de Referência. Nessa mesma reunião será definido o cronograma de implantação/migração da solução;

6.9.1.3.1. O licenciamento da solução deverá ser disponibilizado a partir da data de início da execução do cronograma. O Recebimento definitivo fica condicionado à entrega de todos os agentes instalados e licenciados, conforme definido na Reunião de Alinhamento, observadas as considerações dos itens 5.1.2.2.4.1. e 5.1.2.2.4.2.

6.9.1.4. A implantação inicial consiste em aplicar as regras de acordo com a Politica de Segurança da Informação do Tribunal de Justiça do Estado do Piauí, podendo ainda serem definidas e criadas novas regras de acordo com as necessidades informadas pela equipe técnica de TI do TJPI, sempre levando em consideração as melhores práticas estabelecidas no mercado;

6.9.1.4.1. É de responsabilidade da CONTRATADA a implantação da solução contemplando todos os itens apresentados neste Termo de Referência ou selecionados de acordo com as necessidades apresentadas pela equipe técnica do TJPI, incluindo todas as configurações necessárias à implantação e integração da solução ao ambiente de segurança do TJPI, sempre com acompanhamento e apoio da equipe técnica do TJPI.

6.9.1.4.1.1 A instalação dos agentes da solução contratada nos endpoints do PJPI deverá ser feito em conjunto com a equipe da STIC.

6.9.1.4.2. Todas as configurações a serem feitas e aplicadas pela CONTRATADA no ambiente de infraestrutura do TJPI deverão ser previamente apresentadas para a equipe técnica da CONTRATANTE no momento da implantação/configuração da solução.

6.9.1.4.2.1. Tais configurações só poderão ser aplicadas com o aval da equipe técnica de TI do TJPI;

6.9.1.5. No caso de inadequação técnica, o Tribunal de Justiça do Estado do Piauí encaminhará à CONTRATADA os critérios inadequados encontrados nos serviços no prazo máximo de 03 (três) dias úteis;

6.9.1.6. A CONTRATADA deverá avaliar, e, após confirmação das inadequações, deverá ser agendada com o Tribunal de Justiça do Estado do Piauí a manutenção para efetuar as devidas correções;

6.9.1.7. Durante todo o processo de implantação a CONTRATADA deve prestar suporte em eventuais dificuldades que venham a surgir, sem custo adicional para a CONTRATANTE;

6.9.1.8. Todas as configurações de implantação serão revisadas pelos analistas do Tribunal de Justiça do Estado do Piauí, antes de serem inseridas na nova solução;

6.9.1.9. Todas as etapas das configurações da nova solução deverão ser supervisionadas pela equipe de TI do tribunal;

6.9.1.10. O planejamento da implantação/migração deverá ser acordado na reunião de alinhamento do projeto e apresentado antes do início das atividades à equipe responsável da CONTRATANTE, incluindo mas não se limitando, a análise do ambiente de infraestrutura atual do Tribunal de Justiça do Estado do Piauí e o planejamento da implantação da nova solução.

6.9.1.11. Ao final da implantação e configuração da solução, deverá ser realizado o repasse de informações hands-on, apresentando as configurações implementadas na solução, de no mínimo 8 (oito) horas.

6.9.1.12. Todas as despesas referentes aos serviços de implantação serão de responsabilidade da CONTRATADA.

7. FORMA DE PAGAMENTO:

7.1. O pagamento obedecerá, para cada fonte diferenciada de recursos, a estrita ordem cronológica das datas de suas exigibilidades, conforme determinado pela IN TCE/PI nº 02/2017 e art.5º da Lei 8.666/93.

7.2. O pagamento será efetuado pela Administração, em moeda corrente nacional, por Ordem Bancária, acompanhado dos seguintes documentos, remetidos pelo Fiscal de Contrato ou pela Comissão de Fiscalização:

a) Termo de Recebimento Definitivo ou Recibo, devidamente preenchido e assinado;

b) Apresentação da Nota Fiscal com dados bancários, fatura ou documento equivalente, atestado pelo setor competente;

c) Cópia do Contrato Administrativo ou da Ordem de Fornecimento; e

d) Cópia da Nota de Empenho;

e) Prova de regularidade perante o Instituto Nacional do Seguro Social – INSS;

f) Prova de regularidade do FGTS;

g) Prova de regularidade com a Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede e dívida ativa;

h) Certidão Negativa de Débitos Trabalhistas; e

g) Consulta ao Cadastro de Empresas Inidôneas e Suspensas - CEIS.

7.3. As certidões extraídas do Sistema de Cadastramento Unificado de Fornecedores – SICAF substituirão os documentos relacionados nas letras e, f, g e h, nos termos da Instrução Normativa nº 03/2018 - SEGES/MPDG.

7.4. A Nota Fiscal/Fatura deverá ser emitida pela licitante vencedora obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e das propostas, não se admitindo Notas Fiscais/Faturas emitidas com outros CNPJ, mesmo aquelas de filiais ou da matriz. As Notas Fiscais deverão conter discriminação idêntica à contida na respectiva Nota de Empenho.

7.5. O banco ao qual pertence à conta da empresa deve ser cadastrado no sistema do Banco Central do Brasil, para que seja possível a compensação bancária, na qual o SOF / FERMOJUPI creditará os pagamentos a que faz jus a empresa contratada.

7.7. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência.

7.7. Na existência de erros, omissões ou irregularidades, a documentação será devolvida à empresa contratada/fornecedora, para as correções devidas, passando o novo prazo para pagamento a ser contado a partir da data da apresentação dos documentos corrigidos.

7.8. Não haverá, em hipótese alguma, pagamento antecipado.

.7.9. No caso de eventuais atrasos de pagamento incidirão correção monetária e juros moratórios, desde que a CONTRATADA não tenha concorrido de alguma forma para o fato ensejador da delonga.

7.10. Fica convencionado que a correção monetária e os encargos moratórios serão calculados entre a data do adimplemento da parcela e a do efetivo pagamento da nota fiscal/fatura, com a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,0001638, assim apurado:

I = TX/365 I = 0,06/365 I = 0,0001644

TX = Percentual da taxa anual = 6%.

7.11. A correção monetária será calculada com a utilização do índice IPCA do IBGE.

7.12. No caso de atraso na divulgação do IPCA, será utilizada a última publicação conhecida deste índice, liquidando-se a diferença correspondente tão logo seja divulgado o índice definitivo.

7.13. Caso o IPCA estabelecido venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação então em vigor.

7.14. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial.

7.15. Qualquer atraso ocorrido na apresentação da nota fiscal, ou dos documentos exigidos como condição para pagamento por parte da CONTRATADA importará em prorrogação automática do prazo de vencimento da obrigação do CONTRATANTE.

8. DAS PENALIDADES ADMINISTRATIVAS

8.1. Comete infração administrativa nos termos da Lei nº 8.666/93 e da Lei nº 10.520/02, a licitante vencedora que:

8.1.1. Não Celebrar o Contrato;

8.1.2. Deixar de entregar ou apresentar documentação falsa exigida para o certame;

8.1.3. Ensejar o retardamento da execução de seu objeto;

8.1.4. Não mantiver a proposta;

8.1.5. Falhar ou fraudar na execução do contrato;

8.1.6. Comportar-se de modo inidôneo;

8.1.8. Cometer fraude fiscal;

8.2. Para os fins do item 4.1.2.10.1.6, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei n.º 8.666/1993.

8.3. A Contratada que cometer qualquer das infrações discriminadas acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções, tomando por base o Anexo I:

a) Advertência, em caso de faltas ou descumprimentos de regras contratuais que não causem prejuízo ao CONTRATANTE;

b) Multa:

b.1.) Multa moratória de até 15% (quinze por cento) sobre o valor da parcela inadimplida, no caso de atraso injustificado, até o limite de 30 (trinta) dias;

b.2) Multa compensatória de até 30% (trinta por cento) sobre o valor do contrato, no caso de inexecução total do objeto, configurada após o nonagésimo dia de atraso;

b.3) Em caso de inexecução parcial, aplicar-se-á a multa compensatória no mesmo percentual do subitem anterior, de forma proporcional à obrigação inadimplida;

c) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

e) Impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste Contrato e demais cominações legais.

8.4. As sanções previstas nas alíneas "a", "c" e "d" do subitem anterior poderão ser aplicadas cumulativamente com a pena de multa, de acordo com o Anexo I deste Termo.

8.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

8.5.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

8.5.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

8.5.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

8.6. Após o nonagésimo dia de atraso, o TJ/PI poderá rescindir o contrato, caracterizando-se a inexecução total do seu objeto.

8.8. A aplicação de qualquer das penalidades previstas neste Termo de Referência ou em Contrato Administrativo realizar-se-á através de processo administrativo no qual será assegurado o contraditório e ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993.

8.8. Na aplicação das sanções, a autoridade competente levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8.9. O valor da multa aplicada será descontado da garantia prestada, se houver, ou descontado de pagamentos eventualmente devidos à CONTRATADA. Na inexistência destes, será pago mediante depósito bancário em conta a ser informada pela CONTRATANTE ou cobrada judicialmente.

8.10. Se o valor do desconto nos moldes do item anterior for insuficiente, fica a contratada obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

8.11. Esgotados os meios administrativos para cobrança do valor devido pela contratada ao TJPI, o débito será encaminhado para inscrição em dívida ativa.

8.12. Do ato que aplicar a penalidade caberá recurso no prazo de 05 (cinco) dias úteis a contar da ciência da intimação do ato.

8.13. Da declaração de inidoneidade para licitar ou contratar com a Administração Pública caberá pedido de reconsideração dirigido ao Presidente do TJPI no prazo de 10 (dez) dias úteis da intimação do ato.

8.14. Serão publicadas no Diário da Justiça do TJPI as sanções administrativas previstas, inclusive a reabilitação perante a Administração Pública.

ANEXO I

Infrações, graus, multas e penalidades

Item	Infração	Grau	Multa
1	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que sejam consideradas leves	1	Moratória
2	Não entrega de documentação simples solicitada pelo CONTRATANTE	1	Moratória
3	Atraso parcialmente justificado na entrega até 30 dias.	2	Moratória
4	Atraso parcialmente justificado na entrega acima de 30 dias até 60 dias.	3	Moratória
5	Atraso parcialmente justificado ou injustificado na entrega acima de 60 dias.	4	Compensatória
6	Descumprimento de outros prazos, previstos do TR	2	Moratória
7	Erros de execução do objeto	3	Moratória
8	Desatendimento às solicitações do CONTRATANTE	3	Moratória
9	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais anteriores, que seriam consideradas médias	3	Moratória
10	Execução imperfeita do objeto	3	Moratória
11	Não manutenção das condições de habilitação e de licitar e contratar com a Administração Pública durante a vigência contratual	4	Compensatória
12	Não entrega de documentação importante solicitada pelo CONTRATANTE	4	Compensatória
13	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que seriam consideradas graves	4	Compensatória
14	Inexecução parcial do Contrato	4	Compensatória
15	Descumprimento da legislação (legais e infralegais) afeta à execução do objeto (direta ou indireta)	5	Compensatória
16	Cometimento de atos protelatórios durante a execução visando adiamento dos prazos contratados	5	Compensatória
17	Inexecução total do Contrato	5	Compensatória

Grau	Advertência - 1ª Ocorrência	Mora moratória Valor Mensal	Multa Compensatória	Impedimento Prazo
1	Sim	Não	Não	Não
2	Não	1% a 4,9% por ocorrência ou contrato	1,5% a 4,9% por ocorrência ou contrato	Mínimo: 1 mês Máximo: 2 anos
3	Não	5% a 8,9% por ocorrência ou contrato	8,0% a 14,9% por ocorrência ou contrato	Mínimo: 6 meses Máximo: 3

				anos
4	Não	9% a 11,9% por ocorrência ou contrato	15,0% a 24,9% por ocorrência ou contrato	Mínimo: 3 anos Máximo: 5 anos
5	Não	12% a 15% por ocorrência ou contrato	25% a 30% por ocorrência ou contrato	Mínimo: 4 anos Máximo: 5 anos

ANEXO II
MODELO DE PROPOSTA DE PREÇO

Nome da Solução	Item	Quantidade	Valor Unitário	Valor Total
Solução de ENDPOINT XDR	Cortex XDR Pro por endpoint. Subscrição	4500		
	Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição	4500		
	Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro	1		
TOTAL				

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Analista de Sistemas / Desenvolvimento**, em 17/12/2021, às 12:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fabiano Galeno da Costa Pereira**, **Analista de Sistemas / Desenvolvimento**, em 17/12/2021, às 12:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Natanael Henrique Corrêa**, **Técnico em Informática**, em 17/12/2021, às 12:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Ernani Moura Lima**, **Chefe da Seção de Segurança da Informação**, em 17/12/2021, às 13:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **2931266** e o código CRC **0DD380B7**.

Glossário Nº 1/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

ADD-ON HOST INSIGHT	Um módulo complementar para Cortex XDR. O Host Insights combina gerenciamento de vulnerabilidade, inventário de host e um poderoso recurso de pesquisa e destruição para ajudá-lo a identificar e conter ameaças.
ANTIVÍRUS	Programas informáticos desenvolvidos para prevenir, detectar e eliminar vírus de computador.
AV COMPARATIVES	Organização independente de testes de softwares de segurança.
BACKDOOR	É uma porta, normalmente secreta, que permite o acesso ao sistema e seu controle remoto.
BITLOCKER	É um sistema de Criptografia do Windows, presente em versões do Windows Vista, Windows 7, Windows 8 e no Windows 10. Consiste em codificar partições do HDD, protegendo seus documentos e arquivos do computador contra o acesso não autorizado.
CORTEX XDR	Nome geral da solução de XDR da Palo Alto Networks.
CORTEX XDR PRO	Há duas Versões do Cortex XDR, a Prevent e a Pro. Esta última possui mais funcionalidades.
CVE	Sigla inglesa para Vulnerabilidades e Exposições Comuns, é uma lista pública de falhas de **segurança**.
EDR	É uma sigla inglesa para Endpoint Detection and Response, sendo traduzida como detecção e resposta de endpoint. É uma tecnologia que monitora e responde continuamente para mitigar ameaças cibernéticas nos dispositivos protegidos.
ENDPOINT	Endpoint também significa ponto de extremidade. Um endpoint é um dispositivo final conectado à uma rede de comunicações, podendo ser desde computadores e smartphones até câmeras de vigilância e dispositivos IOT.
EXPLOIT	É um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto no software ou hardware de um computador ou outro eletrônico.
FILELESS	O malware sem arquivo é uma variante do software malicioso relacionado ao computador que existe exclusivamente como um artefato baseado na memória do computador, ou seja, na RAM.
FILEVAULT	É um programa de criptografia de disco no Mac OS X 10.3 e posterior.
FIRMWARE	É uma classe específica de software de computador que fornece controle de baixo nível do dispositivo.
FORRESTER WAVE	Organização independente que tem por finalidade testar e comparar soluções de tecnologia.
GARTNER	É uma empresa de consultoria que desenvolve o estudo de tecnologias e testes de soluções tecnológicas.
HANDS ON	Expressão comumente usada em empresas. Significa primariamente pronta disposição do funcionário para qualquer necessidade da empresa, ou, em outras palavras, pró-atividade. "Hands-on" refere-se, também, à expressão "mão na massa" ou "aprender fazendo".
MACHINE LEARNING	Diz-se de capacidade de aprendizado de um determinado programa, conseguindo se alimentar automaticamente em vez de manualmente por inteligência humana.
MALWARE	Também conhecido por código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações.
MITTRE ATT&CK	Organização independente de testes de softwares de segurança.
NDR	Network Detection and Response (ou Detecção e Resposta de Rede, em português) usa uma combinação de machine learning, advanced analytics e detecção baseada em regras para detectar atividades suspeitas em redes corporativas.

NEXT-GENERATION	Referência feita a qualquer produto ou solução inovadora, que busca diferenciais e avanços tecnológicos ainda não alcançados pelas soluções tradicionais.
NGFW	Os firewalls de próxima geração (NGFWs) são firewalls de inspeção profunda de pacotes que vão além da inspeção e bloqueio de portas/protocolos adicionando inspeção no nível do aplicativo, prevenção de intrusões e absorvem inteligência de fora do firewall.
NTA	Network Traffic Analysis (NTA) é a ferramenta capaz de coletar e analisar o tráfego de redes corporativas para identificar e responder a ataques cibernéticos, permitindo que os mesmos sejam neutralizados.
RANSOMWARE	É um tipo de malware que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados.
TCO	É uma métrica de análise que tem como objetivo calcular os **custos** de vida e de aquisição de um produto, ativo ou sistema.
TIC	Tecnologia da Informação e Comunicação.
TRAPS	Antiga solução de endpoint da empresa Palo Alto Networks.
TROUBLESHOOTING	Sinônimo da língua inglesa para resolução de problemas, podendo seguir determinadas estratégias a fim de se obter melhor resultado.
WORMS	Em computação se refere a um programa independente, do tipo malware, que se replica com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acessá-lo.
XDR	Extended detection and response oferece detecção e resposta estendidas, sendo uma tecnologia de segurança cibernética que monitora e reduz as ameaças à segurança cibernética através do monitoramento de diversas camadas de segurança de forma conjunta.

Documento assinado eletronicamente por **Natanael Henrique Corrêa**, **Técnico em Informática**, em 25/08/2021, às 08:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Analista de Sistemas / Desenvolvimento**, em 25/08/2021, às 08:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Ernani Moura Lima**, **Chefe da Seção de Segurança da Informação**, em 25/08/2021, às 09:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **2645319** e o código CRC **307E37F7**.