Estudos Preliminares Nº 47/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (ART. 14)

1. Requisitos da contratação

De início, mostra-se necessário definir, com base na necessidade do TJPI, quais as principais características que a solução deve atender. Nesse sentido e em atenção à Resolução Nº 182/2013 do CNJ, procede-se à definição das necessidades mínimas que se espera atender com a aquisição da solução de TIC objeto deste Estudo Preliminar.

1.1 Necessidades do negócio

Com vias a melhor instruir o processo em epígrafe, bem como subsidiar a confecção do Termo de Referência, procede-se à listagem das principais necessidades com suas respectivas funcionalidades a serem atendidas com a contratação pretendida.

1.1.1. Necessidade: Adquirir ferramenta com características estendidas de detecção e resposta a incidentes de segurança.

1.1.1.1. Funcionalidade 1: Salvaguardar dados e informações sensíveis existentes no ambiente corporativo do TJPI;

1.1.1.2. Funcionalidade 2: Proteger as estações de trabalho do TJPI de ameaças oriundas de vírus, *worms*, *ransomwares*, *backdoors* e *malwares* em geral;

1.1.1.3. Funcionalidade 3: Responder o mais prontamente possível às ameaças virtuais detectadas;

1.1.1.4. Funcionalidade 4: Aumentar a visibilidade e a detecção de incidentes ao nível da rede correlacionando estes eventos com os dos endpoints;

1.1.1.5. Funcionalidade 5: Padronizar e centralizar a gestão da ferramenta de antivírus no âmbito do TJPI.

1.1.2. Atores envolvidos: para o projeto em epígrafe ficam destinadas as seguintes partes fundamentais:

1.1.2.1. Gerente de projetos da CONTRATANTE: servidor indicado pela autoridade competente do TJPI para liderar o projeto de contratação da solução bem como atestar a regularidade das fases pertinentes e manter contato direto com o preposto da CONTRATADA.

1.1.2.2. Gerente de projetos da CONTRATADA: preposto indicado pela empresa fornecedora da solução com funções de gerência e/ou liderança que deverá manter contato direto com o gerente de projetos da CONTRATADA em todas as fases do projeto com o fito de garantir a regularidade da aquisição.

1.1.2.3. Analistas de TIC de Infraestrutura e Segurança da Informação da STIC com a função de descrever os requisitos técnicos bem como testar e homologar a conformidade do fornecimento da solução em aderência aos padrões descritos.

1.2. Requisitos não funcionais/tecnológicos

1.2.1. Requisitos de capacitação:

Como medida de eficiência, recomenda-se que seja feito o repasse de conhecimento para as equipes de infraestrutura e segurança da STIC, a ser realizado após a implantação da solução, do tipo Hands On, com no mínimo 08 (oito) horas de duração, contemplando as principais funcionalidades da solução, bem como as configurações específicas que foram implementadas no ambiente.

1.2.2. Requisitos legais:

Esta contratação busca atender as necessidades do PJPI, obedecendo rigorosamente às legislações federal e estadual pertinentes, às Resoluções do CNJ, bem como aos instrumentos legais emitidos pelos órgãos avaliadores de conformidade como a Associação Brasileira de Normas Técnicas – ABNT, o Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO, Instituto Brasileiro de Meio Ambiente – IBAMA, dentre outros.

No que tange à legislação específica, não fora encontrada nenhuma observância obrigatória para o projeto em epígrafe.

1.2.3. Requisitos de manutenção:

- A execução contratual será acompanhada e fiscalizada por representantes da contratante, que poderá utilizar-se da contratação de terceiros para assisti-la e subsidiá-la de informações pertinentes a essa atribuição, em consonância com as disposições do art. 67 da Lei nº 8.666/1993.
- A fiscalização não exclui nem reduz a responsabilidade das empresas contratadas pelos danos causados à contratante ou a terceiros decorrentes de ato ilícito na execução do contrato. Além disso, a ocorrência de irregularidades não implica em corresponsabilidade da contratante.
- A avaliação da qualidade e da adequação dos serviços ocorrerá a cada entrega de produtos previstos nas Ordens de Serviço, e será realizada pelo Fiscal Técnico do Contrato com base nos indicadores definidos no Termo de Referência, a partir dos registros das demandas mantidos pela STIC. Para avaliar a qualidade dos serviços prestados, o TJPI poderá utilizar os registros gerados por outras empresas contratadas.
- Os serviços executados deverão atender aos níveis de serviços estabelecidos pelo TJPI, para cada

tipo de serviço contratado. As empresas contratadas estarão sujeitas, garantido o contraditório e a ampla defesa, às sanções administrativas em função dos indicadores obtidos abaixo da faixa de ajuste. A aplicação dos ajustes do pagamento não exclui a aplicação de multas e sanções previstas neste documento.

1.2.4. Requisitos temporais:

1.2.4.1. Planejamento do processo de aquisição por parte da equipe de planejamento da contratação: para garantir eficiência no processo de contratação, ficam definidos um prazo máximo de 15 (quinze) dias para cada uma das seguintes fases:

i. Planejamento interno da contratação a ser realizado pela equipe de contratação;

ii. Tramitação processual, incluindo aprovação da demanda por parte da autoridade competente;

iii. Formulação do edital de licitação e aprovação da minuta por parte da autoridade máxima do TJPI;

iv. Realização do certame licitatório e contratação da empresa vencedora.

1.2.4.2. 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.

1.2.4.3. 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.

1.2.4.4. 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 5.1.3.1. 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.

1.2.4.5. 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.

1.2.5. Requisitos de segurança

A solução deve estar em conformidade com a Política de Segurança da Informação do Tribunal de Justiça do Piauí, bem como com os procedimentos e documentações exigidas.

Todas as informações consideradas sensíveis pelo TJPI deverão ser resguardadas por parte da CONTRATADA não sendo permitido, em hipótese alguma, o compartilhamento, cópia, retirada, reprodução, carga, levantamento, entre outros, de informações oriundas dos sistemas informatizados e/ou bancos de dados institucionais sem a devida autorização prévia e expressa por parte da autoridade competente do TJPI.

São consideradas sensíveis, para fins de aplicação do item anterior, aquelas informações que por sua natureza são consideradas de interesse confidencial, restrita ou sigilosa como, por exemplo:

- Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto ser divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo TJPI a tais documentos.
- Resultados, parciais ou totais, sobre produtos gerados.
- Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações.
- Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do TJPI e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões "beta" de quaisquer programas, dentre outros.
- Documentos relativos à lista de usuários do TJPI e seus respectivos dados, armazenados sob qualquer forma.
- Metodologias e ferramentas de serviços, desenvolvidas pelo TJPI.
- Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do TJPI, sejam eles executados interna ou externamente.
- Parte ou totalidade dos dados ou informações armazenados nas bases de dados que subsidiam os sistemas de informações do TJPI, sejam elas residentes interna ou externamente.
- Circulares e comunicações internas do TJPI.
- Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo TJPI.

1.2.6. Requisitos sociais, ambientais e culturais

A fabricante da solução deverá atender aos critérios de sustentabilidade ambiental de que trata a Instrução Normativa SLTI/MPOG nº 01/2010, no que couber, quanto ao uso de materiais, observando que esses sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme Normas ABNT NBR – 15448-1 e 15448-2.

Deverão ser observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares, se aplicável.

1.3. Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

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, integrando-se com as soluções de segurança já implementadas.

1.3.1. Levantamento das alternativas disponíveis no mercado de TIC

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 existentes.

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 pela 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), quando traz 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 detecção e resposta a incidentes (EDR), chegando a soluções ainda mais completas para ambientes corporativos, integrando diversas camadas de segurança como rede, firewall, IoT, nuvem e Endpoints (XDR).

1.3.2. Contratações Públicas Similares (Art. 14, I, b)

Pelos motivos que serão explicitados, as contratações públicas consideradas como similares foram apenas as da fabricante Palo Alto Networks.

A fabricante Palo Alto Networks possuía uma solução de proteção EDR conhecido como TRAPS, porém este foi remodelado e atualizado passando a ser conhecido como **Cortex XDR**, devido a ter uma abrangência maior e ter ganho novas funcionalidades.

As soluções da Palo Alto são amplamente aceitas no mercado, estando entre as melhores posições nos laboratórios de pesquisas independentes, como Forrester Wave, Gartner, Mitre Att&ck, AV Comparatives, dentre outros.

A exemplo, seguem duas contratações públicas encontradas:

ÓRGÃO	OBJETO
FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA	REGISTRO DE PREÇOS PARA AQUISIÇÃO DE TRANSCEIVERS DA FABRICANTE PALO ALTO NETWORKS PARA SEREM UTILIZADOS EM EQUIPAMENTOS DO TIPO FIREWALL NOVOS E LEGADOS E SOFTWARE PARA EXPANSÃO DA INFRAESTRUTURA DE DE SEGURANCA

– IBGE PREGÃO ELETRÔNICO Nº 08/2021	INFRAESTRUTURA DE DE SEGURANÇA.
MINISTÉRIO DA EDUCAÇÃO INSTITUTO NACIONAL DE EDUCAÇÃO DE SURDOS-INES PREGÃO ELETRÔNICO N° 28/2017	O PRESENTE TERMO DE REFERÊNCIA TEM POR OBJETO A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO AVANÇADA PARA ENDPOINTS COM GERENCIAMENTO DA MARCA TRAPS DA FABRICANTE PALO ALTO NETWORKS, CONTEMPLANDO IMPLANTAÇÃO, SUPORTE E TREINAMENTO, VISANDO ATENDER A NECESSIDADES NA ÁREA DE SEGURANÇA DA INSTITUIÇÃO NA ÁREA DE TI. A OBTENÇÃO DESTE RECURSO TEM POR FINALIDADE FORNECER SUPORTE NECESSÁRIO AS ATIVIDADES FINALÍSTICAS DO INSTITUTO NACIONAL DE EDUCAÇÃO DE SURDOS – INES.

1.3.3 A Disponibilidade de Solução de Tecnologia da Informação e Comunicação similar em outro órgão ou entidade da Administração Pública; (Art. 14, II, a)

Trata-se de serviço exclusivamente disponibilizado pelas empresas parceiras da fabricante e detentora dos direitos sobre os produtos, portanto, não está disponível nos órgãos públicos para cessão de uso.

1.3.4 Portal do Software Público Brasileiro (Art. 14, II, b)

Não se aplica. Uma solução de antivírus não é apenas um software que possa ser encontrado num determinado repositório, seja este público ou privado. O software é apenas o meio através do qual é prestado um serviço com atualização constante.

1.3.5 Alternativa no Mercado de TIC (Art. 14, II, c)

Dentre as principais soluções de XDR, podemos citar os produtos das fabricantes Trend Micro, Cynet, CrowdStrike, Microsoft, SentinelOne, Cybereason, Broadcom, Cisco, Mandiant, VMware, McAfee e Sophos, além da solução da Palo Alto Networks, objeto da contratação em análise. Em maior ou menor grau, todas elas pretendem oferecer soluções integradas cada vez mais abrangentes para garantir a segurança de empresas e instituições públicas.

1.3.6 Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d)

Não se aplica, por não se tratar de desenvolvimento de sistemas.

1.3.7 Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e)

Não se aplica por não envolver necessidades de certificação digital.

1.3.8 Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

Não se aplica. O objeto não trata de desenvolvimento de sistemas.

2. Estimativa do Valor da Contratação

A tabela abaixo resume os custos totais da solução, baseada na Pesquisa de Preços 79 (SEI 2573496):

Quantidade a ser Registrada.				
Nome da Solução	**Item**	**Quantidade**	**Valor Unitário**	**Valor Total**
Solução de ENDPOINT XDR	Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	3000	R$ 327,15	R$ 981.460,00
	Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	3000	R$ 50,36	R$ 151.080,00
	Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro	1	R$ 166.205,00	R$ 166.205,00
TOTAL				R$ 1.298.745,00

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

3. Justificativa da solução escolhida (art. 14, IV)

Esta aquisição revela-se como uma extensão da segurança em camadas já existente no TJPI, proporcionando uma melhoria significativa em termos de segurança e trazendo benefícios como integração, redução de custos e melhor aproveitamento do investimento feito, como ficará demonstrado a seguir.

O objeto desta contratação é a aquisição de uma solução de segurança avançada de endpoints, 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 estende a detecção à outras fontes de dados além do Endpoint, diferenciado-se de proteções como as de EDR (Endpoint Detection and Response - EDR) que oferecem detecção e resposta de incidentes somente ao nível do Endpoint.
A proteção provida pelas soluções de XDR revela-se como uma evolução tecnológica e uma mudança de abordagem no tratamento da segurança corporativa, mostrando-se a mais avançada em termos de proteção de Endpoint, sem, no entanto, se limitar a ela, abrangendo também outras camadas de segurança, até então tratadas de forma isolada, o que reduzia a visibilidade e dificultava a detecção de um incidente de segurança por prescindir de grande esforço humano para realizar a correlação entres os eventos das várias camadas.

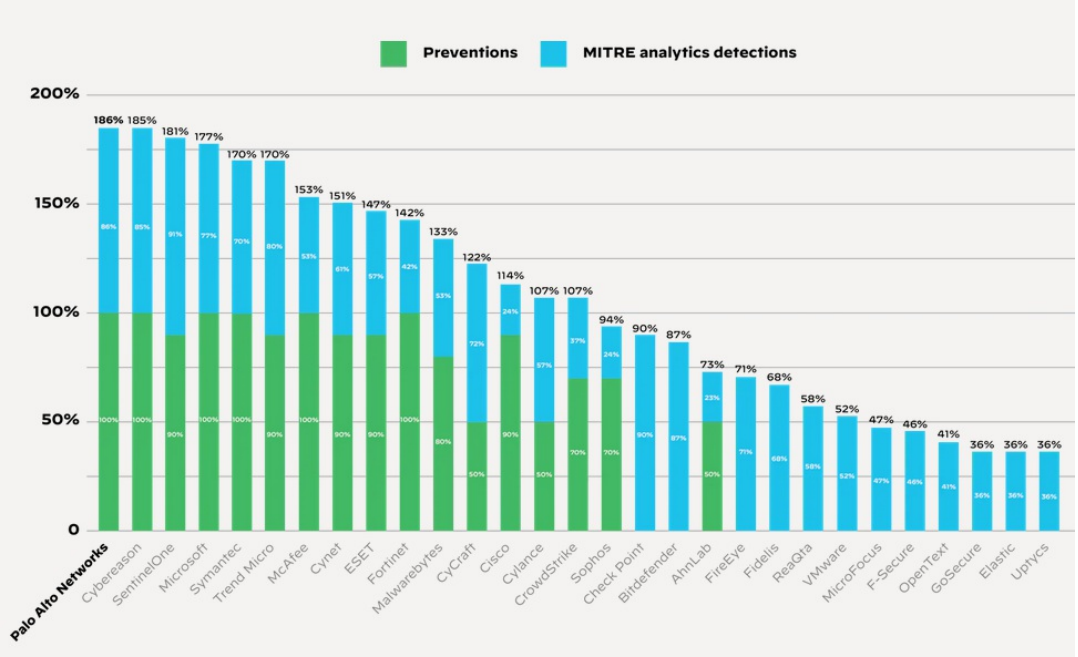
Dentre as principais soluções de XDR, podemos citar os produtos das fabricantes Trend Micro, Cynet, CrowdStrike, Microsoft, SentinelOne, Cybereason, Broadcom, Cisco, Mandiant, VMware, McAfee e Sophos, além da solucão da Palo Alto Networks, objeto da contratação em análise. Em maior ou menor grau, todas elas pretendem oferecer soluções integradas cada vez mais abrangentes para garantir a segurança de empresas e instituições públicas. Ocorre que, no mesmo ritmo em que essas soluções progridem, também aumentam e se diversificam as ameaças virtuais.

Na prática, isso significa que as melhores soluções são aquelas que estão em evolução constante, visão mais abrangente e sofisticação dos métodos de detecção, mostrando-se capazes de prever antecipadamente às novas tendências, o que nos leva à busca de uma solução reconhecida no mercado de segurança da informação, que além de passar por todo tipo de testes do mundo real, sejam capazes de prover a **melhor proteção** possível no panorama atual.

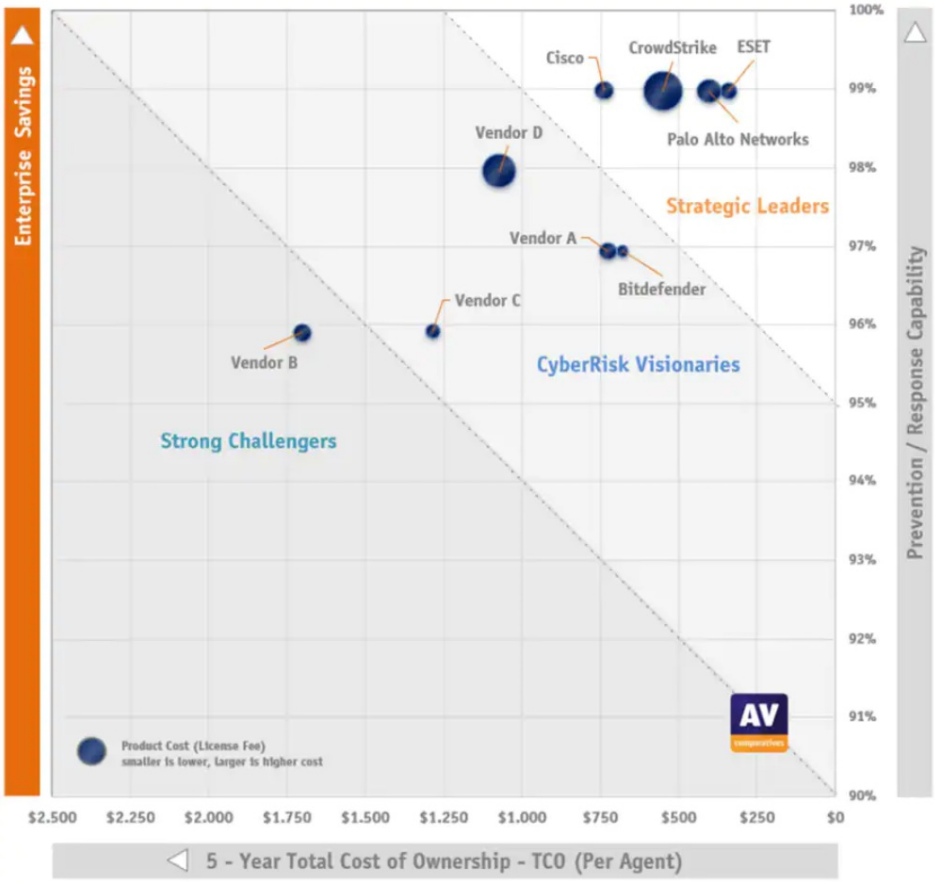
Com o intuito de melhor avaliar a competência tecnológica das soluções disponíveis no mercado, o que demanda tempo, testes exaustivos, conhecimento especializado e dedicação exclusiva à este propósito, recorremos aos estudos já feitos pelos laboratórios de pesquisa independentes Mittre Att&ck, AV Comparatives e Forrester Wave.

Importante destacar que a solução da Palo Alto Networks, assim como outras soluções, em sua maioria, são evoluções das soluções de EDR. Nas imagens abaixo o comparativo é feito com proteções de EDR, incluindo também algumas proteções de XDR.

A seguir é mostrado o resultado de um estudo feito pelo Mitre Att&ck no ano de 2021, com foco nas técnicas, táticas e procedimentos utilizados por ameaças que visam instituições financeiras. Importante destacar que é o terceiro ano consecutivo que a Palo Alto é bem avaliada nos estudos do Mitre Att&ck. A parte azul da barra mostra, em percentual, a capacidade de detecção das soluções analisadas, já a parte verde mostra a capacidade de prevenção.



Na figura abaixo vemos o resultado do estudo feito pelo AV Comparatives em Dezembro de 2020, onde mostra a solução da Palo Alto Networks nas melhores colocações, por possuir capacidade de resposta aos incidentes próxima de 100%. Este estudo também mostra que a solução da Palo Alto Networks possui grande valor agregado. Isso é medido de acordo com os tempos e capacidade de resposta e prevenção aos incidentes. Também é mostrado que a solução tem uma excelente relação **custo/benefício**, por possuir um dos menores valores do custo total da posse (TCO), que é uma estimativa financeira de avaliação dos custos diretos e indiretos relacionados à compra e operação da solução ao longo do tempo (5 anos no estudo).



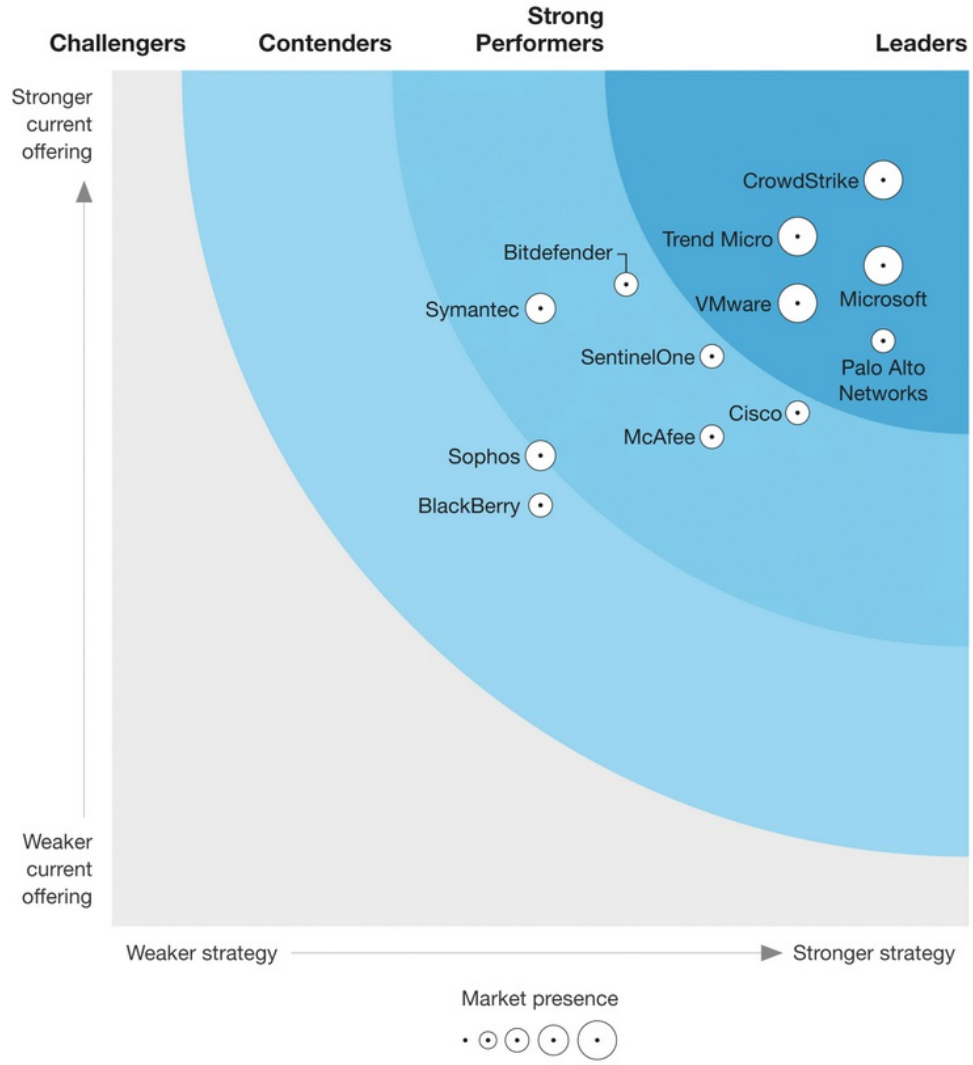
Na figura seguinte vemos a comparação de soluções de proteção de endpoint de vários fabricantes, feitos pela Forrester Wave no ano de 2021. Mais uma vez a Palo Alto Networks figura entre os líderes nesse nicho de mercado.

FORRESTER®

THE FORRESTER WAVE™

Endpoint Security Software As A Service

Q2 2021



É notório que a solução de XDR da Palo Alto Networks figura sempre entre as **melhores posições** nos testes efetuados por estes laboratórios, que simulam sequências de ataques do mundo real, reunidos em estudos dos grupos mais sofisticados de ameaças persistentes avançadas do mundo.

Apesar de existirem outras soluções de XDR bem avaliadas e o quesito competência técnica representar um fator preponderante na escolha da solução, ele não é o único critério a ser avaliado, sendo necessário observar o cenário proposto para uma perfeita adequação ao ambiente corporativo.

Devido à existência de uma solução de segurança já implantada no TJPI (NGFW Palo Alto Networks) esta aquisição se coloca como um complemento dessa segurança, tendo como foco principal a proteção dos endpoints, ao mesmo tempo que se integra com a solução já implantada, promovendo uma plataforma de segurança mais eficiente e eficaz.

De forma a esclarecer melhor o objetivo da contratação é importante fazer a seguinte comparação entre o que a solução já implantada no TJPI oferece e as melhorias que a solução objeto desta contratação vai proporcionar ao ambiente computacional do TJPI.

Proteção	NGFW Palo Alto já implantado no TJPI sem Cortex XDR Pro	NGFW Palo Alto integrado com Cortex XDR Pro
Sandbox	X	X
Antivírus	Limitado	X
Ransomware	Limitado	X
Machine Learning	X	X
Inteligência Artificial		X
Malwares	Limitado	X

conhecidos	Limitado	X
Malwares desconhecidos	Limitado	X
Filtro de URL	X	X
Vulnerabilidades	Limitado	X
Escalação de privilégios		X
Movimentação Lateral	Limitado	X
Exfiltração de dados	X	X

Como é possível observar na tabela exemplificativa acima, muitos recursos de segurança da informação existentes no órgão possuem abrangência limitada. Isto ocorre porque o firewall (NGFW) atua somente na camada de rede, o que deixa os endpoints sujeitos a infecções por diversos tipos de *malwares*, como *ransomwares*, vírus e scripts que não tenham como origem a rede (dispositivo removível, por exemplo) ou que se limitem ao mesmo segmento de rede, onde o firewall não consegue inspecionar o tráfego. A escalação de privilégios é outro exemplo de ataque que ocorre somente dentro do dispositivo atacado e não pode ser inspecionado pelo firewall.

Para se ter um controle efetivo da segurança é necessário que a solução de proteção dos endpoints seja capaz de se integrar e interagir com a solução existente, sendo um dos principais critérios levados em consideração neste estudo preliminar para a definição de uma solução aderente ao cenário do TJPI.

Há que se considerar ainda a **vantajosidade econômica** obtida em relação à dispensa de aquisição de alguns elementos envolvidos direta ou indiretamente com a solução, como é o caso da sandbox, que é um mecanismo de análise dos arquivos suspeitos em nuvem, onde os arquivos são executados em ambientes de teste a fim de analisar seu comportamento, resultando em um veredito, que revela se o arquivo é malicioso ou não. Não será necessário adquirir esta parte, componente de uma solução de NDR, pois será aproveitada a mesma que já está em funcionamento, licenciada para uso pelo NGFW instalado. Outro caso que dispensará aquisição, por já estar contemplada nesta aquisição é uma ferramenta de SIEM, pois o núcleo da solução já traz esta funcionalidade, sendo suficiente para os agentes de proteção de endpoints e firewall. Caso seja necessário futuramente o uso deste recurso para ferramentas de terceiros, a única necessidade será a de licenciar espaço de armazenamento na nuvem da fabricante para armazenamento dos logs destas ferramentas, como logs de aplicações e de sistemas, por exemplo. Desta feita isso importará em um custo reduzido em relação à aquisição de uma solução específica para este propósito.

Outro fator que não pode ser desprezado quando se trata de integração de soluções de tecnologia, é que as soluções sejam perfeitamente suportadas por um mesmo fabricante, a fim de se evitar problemas de integração e eliminar a possibilidade de que algum dos fabricantes (caso sejam diferentes) se furtem à responsabilidade da resolução dos problemas, imputando a responsabilidade da resolução do problema para a fabricante da outra solução. Esse é um fato comum observado nas contratações de soluções de tecnologia e que deve ser valorizado na contratação da solução mais adequada para suprir as demandas que exigem integração.

Um dos pilares para a escolha de uma solução desse tipo foi propiciar uma forma de simplificar as operações de detecção e resposta de incidentes de forma estendida, evitando tratar os incidentes de forma isolada. Isso representa um ganho de eficiência operacional, pois permite que o mesmo trabalho seja feito por menos pessoas quando comparado ao tratamento dos incidentes das diferentes camadas de segurança de forma isolada. Há uma necessidade menor de esforço humano, o que condiz com o cenário do órgão, por ter uma equipe reduzida para muitas tarefas diferentes. Isso também será um ponto positivo caso seja considerada futuramente a possibilidade de contratação de serviços gerenciados de segurança, pois soluções integradas do mesmo fabricante necessitam de uma equipe menor e evitam a necessidade de treinamento em diversas soluções.

A solução proposta visa, portanto, facilitar o trabalho da equipe, uma vez que permite gerenciar de forma centralizada mais de uma camada de segurança, correlacionando os eventos entre elas, classificando os incidentes em níveis de criticidade diferentes e permitindo priorizar as ações mais importantes. Estas ações, em sua maioria, são feitas de forma automatizada, o que se traduz em economiza de recursos humanos necessários para o desempenho destas funções.

É comum vermos a aquisição das soluções de EDR e NDR ser composta por fabricantes diferentes, no entanto esta abordagem dificulta ou impossibilita a integração entre elas, além de reduzir a visibilidade e abrangência somente às camadas de atuação de cada uma, o que pode deixar pontos cegos na infraestrutura envolvida. Esta aquisição, como está proposta, permite que várias camadas de segurança sejam tratadas dentro de uma interface de gerência centralizada, abrangendo em um primeiro momento as camadas de Endpoint e Rede e possibilitando uma expansão futura para outras camadas de segurança, como as de e-mail e nuvem.

Nesta abordagem, o NGFW da fabricante Palo Alto Networks, já adquirido e implantado no TJPI, atuará como analisador de tráfego de rede, dando à solução proposta a visibilidade da camada de rede, permitindo uma análise conjunta e aprofundada do ambiente corporativo e permitindo acompanhar todo o caminho e modo de operação das possíveis ameaças, se traduzindo em um melhor aproveitamento do **investimento** já feito pelo TJPI.

Com uma solução de segurança com estas características implantadas, o TJPI terá proteção aprimorada contra os mais variados tipos de *malwares* e técnicas utilizadas pelos atacantes, incluindo uma análise aprofundada e rica em detalhes por se integrar com a segurança de rede já implementada, propiciando uma visão ampla e unificada sobre as várias camadas de segurança gerenciadas, abrangendo inicialmente as camadas de Endpoint e Rede, mas possibilitando sua expansão para outras camadas, como o E-mail e Nuvem, por exemplo.

3.1. Solução escolhida: Solução de Proteção avançada de endpoints **Palo Alto Cortex XDR Pro** e serviços de implantação e configuração da solução (incluindo Hands On)

3.2. Descrição (art. 14, IV, a):

- Cortex XDR Pro
    - Recursos de Next-Generation Antivirus para impedir exploits, malwares, ransomwares e ataques fileless que afetam os endpoints;
    - Integrado nativamente ao Palo Alto WildFire para análise de malwares desconhecidos em sandbox sem a necessidade de licenciamento adicional;
    - Recursos de Endpoint Protection para controle do dispositivo, firewall integrado e integração com as ferramentas BitLocker e FileVault para encriptação e decriptação do disco rígido;
    - Recurso de Endpoint Detection and Response para descoberta de ataques através de análises utilizando recursos de Inteligência Artificial e respostas aos incidentes de forma automatizada, coordenada e integrada com o firewall Palo Alto;
    - Utiliza dados/logs obtidos tanto do endpoint quanto do firewall Palo Alto para uma visualização mais completa das ações realizadas e executadas pela ameaça detectada;
    - Recurso de Search and Destroy para realizar a remoção do arquivo malicioso de todos os endpoints, de forma rápida e simples;
    - Recurso de inventário exibindo as informações dos sistemas dos endpoints como aplicações instaladas e serviços em execução permitindo identificar comportamentos suspeitos;
    - Recurso para identificar e quantificar as vulnerabilidades de segurança (CVEs) existentes para as aplicações instaladas nos endpoints.

3.3. Composição da solução (art. 14, IV, a):

- Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses.
- Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses.
- Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro.

3.4. Alinhamento em relação às necessidades (art. 14, IV, 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.

3.5. Benefícios esperados (art. 14, IV, 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.

3.6. Relação entre a demanda prevista e a quantidade a ser contratada (art. 14, IV, d):

A quantidade a ser contratada imediatamente foi considerada tendo como base a quantidade de servidores e estações de trabalho existentes atualmente no parque tecnológico do TJPI. Há previsão de aquisição de telefones móveis corporativos, o que de demandará a contratação de mais licenças posteriormente.

Nome da Solução	Item	QUANTIDADE A SER REGISTRADA	QUANTIDADE A SER CONTRATADA DE IMEDIATO
Solução de ENDPOINT XDR	Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	3000	2700
	Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	3000	2700
	Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro	1	1
	TOTAL	**R$ 1.298.745,00**	

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

orçamento disponível.

4. Necessidades de adequação do ambiente do órgão (art. 14, V):

Tipo	Necessidade
Infraestrutura tecnológica (art. 14, V, a)	Não há.
Infraestrutura elétrica (art. 14, V, b)	Não há.
Logística de implantação (art. 14, V, c)	Após a assinatura do contrato será realizada uma Reunião de Alinhamento com a CONTRATADA para definição das etapas de implantação com os respectivos prazos para entrega e requisitos para aceite.
Espaço físico (art. 14, V, d)	Não há.
Mobiliário (art. 14, V, e)	Não há.
Impacto ambiental (art. 14, V, f)	Não há.

SUSTENTAÇÃO DO CONTRATO (ART. 15)

5. Recursos necessários à continuidade do objeto contratado (art. 15, I)

5.1 Recursos materiais:

A aquisição da solução em epígrafe não necessita de recursos materiais adicionais, já que, o que se quer contratar são licenças de software.

5.2 Recursos humanos:

5.2.1 Recurso 1: Equipe de Infraestrutura e Segurança da Informação da STIC.

5.2.1.1 Função: Operar e manter a solução de TIC em aderência às regras da governança e da alta administração do TJPI.

5.2.1.2 Responsabilidades:

- Manter a solução de TIC em funcionamento, garantindo a segurança dos dados armazenados no ambiente corporativo do TJPI;
- Garantir a segurança, integridade e disponibilidade da informação no TJPI;
- Manter contato direto com a CONTRATADA quando do aparecimento de incidentes e/ou problemas na solução.

5.2.2 Recurso 2: Preposto da CONTRATADA e/ou fabricante da solução.

5.2.2.1 Função: Manter a solução de TIC em perfeito funcionamento independentemente da atuação da Equipe do setor de Infraestrutura e Segurança da Informação da STIC do TJPI.

5.2.2.2 Responsabilidades:

- Atender todas as requisições do TJPI em tempo hábil e de acordo com os níveis de serviço (NSE) acordados;
- Atualizar, sempre que necessário, os softwares integrantes e/ou componentes da solução de TIC;
- Manter a confidencialidade dos dados que tiver acesso em decorrência do contrato a ser firmado.

6. Estratégia de continuidade em eventual interrupção contratual (art. 15. II)

6.1. Evento 1: Descontinuidade da solução de XDR por parte da fabricante.

6.1.1. Ação de contingência: Realizar contratação de nova solução.

6.1.2. Responsável: Equipe de contratação.

6.2. Evento 2: Rescisão contratual por parte da Administração ou da CONTRATADA.

6.2.1. Ação de contingência: Contratar outra empresa que forneça suporte à solução adquirida.

6.2.2. Responsável: Equipe de contratação.

7. Ações para transição e encerramento contratual (art. 15, III)

Ação	Responsável	Data de Início	Data de Fim
Entrega de versões finais dos produtos alvos da contratação (art. 15, inc. III, a)	Contratada	A partir da emissão do termo de recebimento provisório	Até a emissão do termo de recebimento definitivo ou documento semelhante
Transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação (art. 15, inc. III, b)	Contratada	Pelo menos um mês antes da entrada em produção da solução	No máximo uma semana antes da entrada em produção da solução
Devolução de recursos materiais (art. 15, inc. III, c)	Não há necessidade de devolução de qualquer dos materiais contratados.		

Revogação de perfis de acesso (art. 15, inc. III, d)	TJPI	Um mês antes do término do contrato	Até o termo final do contrato
Eliminação de caixas postais (art. 15, inc. III, e)	Não serão criadas caixas postais para atendimento da implantação desta solução.		

8. Estratégia de independência (art. 15, IV)

No que se refere à licença de uso de software, tratando-se de prestador exclusivo, não há possibilidade de definir estratégias de independência tecnológica.

Uma possibilidade seria substituir a solução objeto desta contratação por uma nova solução de segurança. No entanto, continuaria havendo dependência tecnológica da solução substituta, sem falar que outra solução não teria todas as vantagens que foram citadas em relação a esta.

ESTRATÉGIA PARA CONTRATAÇÃO (ART. 16)

9. Natureza do objeto (art. 16, I)

O objeto a ser contratado enquadra-se na categoria de bens/serviços comuns de que tratam a Lei nº 10.520/02 e os Decretos nº 3.555/00 e nº 5.450/05, 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.

10. Parcelamento do objeto (art. 16, II)

Considerando que se trata de solução de proteção de *endpoint* a ser instalada em todos os dispositivos (desktops, notebooks, servidores, etc) pertencentes ao parque tecnológico do TJPI, recomenda-se parcelar o licenciamento de acordo com a disponibilidade orçamentária do TJPI. Nesse sentido, a licitação para registro de preços se mostra ideal para o atendimento da demanda em epígrafe.

11. Adjudicação do objeto (art. 16, III)

Tratando-se de item único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade deste.

12. Modalidade e tipo de licitação (art. 16, IV)

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.

13. Classificação e indicação orçamentária (art. 16, V)

Para atendimento da demanda objeto do presente processo, **sugere-se** a seguinte classificação orçamentária:

ITEM	Objeto	Código	Especificação
1	Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses	• 04.105.02.061.0015.1846 • 04.105.02.061.0015.1847	• REAPARELHAMENTO DA JUSTIÇA DE 1º GRAU • REAPARELHAMENTO DA JUSTIÇA DE 2º GRAU
2	Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses		
3	Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro		

Ressalta-se, outrossim, que a posterior informação por parte da Secretaria de Orçamento e Finanças deste TJPI terá a função de detalhar as naturezas em obediência à legislação vigente.

14. Vigência da garantia e da prestação dos serviços (art. 16, VI)

O Contrato terá vigência de **12 (doze) meses** a contar da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, **limitado a 48 (quarenta e oito) meses**, conforme preconiza o art. 57, inc. II e inc. IV da Lei n° 8.666 de 1993.

15. Equipe de apoio à contratação (art. 16, VII)

Integrante Requisitante	Ernani Moura Lima	Matrícula	30267
E-mail	ernani.lima@tjpi.jus.br	Telefone	(86) 3215-1120
Integrante Técnico	Natanael Henrique Corrêa	Matrícula	5027
E-mail	natanael.henrique@tjpi.jus.br	Telefone	(86) 3215-1120
Integrante Administrativo	Giovanny Lima de Castro	Matrícula	28631
E-mail	giovanny.castro@tjpi.jus.br	Telefone	(86) 3215-1120

16. Equipe de gestão da contratação (art. 16, VIII)

Gestor do Contrato	Agnaldo Abreu Almendra	Matrícula	1055410
E-mail	agnaldo@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Demandante	Eric Barbosa Jales de Carvalho	Matrícula	27683
E-mail	ericjales@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Técnico	Marcus Vinicius Alcantara de Almeida	Matrícula	1635
E-mail	marcus.almeida@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Administrativo	Leandro Sales Lima	Matrícula	27594
E-mail	leandrosales@tjpi.jus.br	Telefone	(86) 3215-1120

ANÁLISE DE RISCOS (ART. 17)

17. Riscos do processo de contratação (art. 17, I)

Risco 1 – Restrição orçamentária					
Probabilidade	Impacto	Ação preventiva	Responsável	Ação de contingência	Responsável
Média	Alto	Priorização deste projeto em detrimento de outras iniciativas	Equipe de Planejamento da Contratação	Reduzir escopo da demanda	Integrante requisitante
Risco 2 – Falhas na especificação dos produtos em relação à capacidade e alinhamento às demandas do órgão					
Probabilidade	Impacto	Ação preventiva	Responsável	Ação de contingência	Responsável
Baixo	Alto	Especificar com minúcia suficiente os requisitos da solução	Equipe de Planejamento da Contratação	Rever o projeto atual e prospectar alteração de configurações para adequação à solução proposta	Integrante requisitante
Risco 3 – Não cumprimento dos prazos acordados					
Probabilidade	Impacto	Ação preventiva	Responsável	Ação de contingência	Responsável
Média	Alto	Monitorar e notificar preventivamente a contratada para que cumpra os prazos	Fiscal técnico	Propor a aplicação de sanções previstas em contrato	Fiscal demandante

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Analista de Sistemas / Desenvolvimento**, em 24/08/2021, às 21:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Natanael Henrique Corrêa**, **Técnico em Informática**, em 24/08/2021, às 21:37, 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 24/08/2021, às 21:38, 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 **2371110** e o código CRC **B681A130**.