PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/SECSTM/DITIN/COTEC

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. OBJETO

Aquisição de Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses com treinamento técnico.

2. DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA DEMANDA

2.1 Requisitos do Demandante

Com a contratação de ferramentas especializadas em segurança da informação, pretende-se colocar o Tribunal em acordo com as recomendações constantes no Manual de Referência de Proteção de Infraestruturas Críticas de TIC, aprovado através da PORTARIA CNJ No 162/2021, e às recomendações constantes na norma ABNT NBR ISO/IEC 27002:2013, no campo de gerenciamento de vulnerabilidades técnicas.

2.2. Quantitativo

Grupo					
Item	Especificação	Unidade	Qtd. Total	Custo Unitário	Total
1	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Licença	2000	R$	R$
2	Treinamento técnico da Solução de Gerenciamento de Vulnerabilidades.	Pessoas	8	R$	R$
Valor Total					**R$**

2.3. Requisitos Técnicos

2.3.1. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo:

2.3.1.1. Ativos em rede;

2.3.1.2. Servidores e Estações de trabalho ou Notebooks;

2.3.1.3. Servidores em Cloud;

2.3.1.4. Contêineres;

2.3.1.5. Aplicações Web e API;

2.3.2. O licenciamento poderá ser flexível, ou seja, não limitado por módulo.

2.3.3. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

2.3.4. A solução deve fornecer alta disponibilidade, com cluster ativo – ativo, no site principal e site backup, com redundância da base de dados entre os sites.

2.3.5. Plataforma de Gestão de Vulnerabilidade em Ativos de Rede e Nuvem.

2.3.6. Controle de Usuários, a ferramenta deve gerenciar e controlar os acessos e usuários

2.3.7. A ferramenta deve possuir Relatórios e Dashboards, a fim de auxiliar o uso e melhorar a experiência do usuário

2.3.8. A ferramenta deve ter Conformidade e Compliance

2.3.9. Possuir Plataforma de Gestão de Vulnerabilidade em Aplicações Web

2.3.10. Possuir Plataforma de Gestão de Vulnerabilidade em Contêineres

2.3.11. Ser capaz de prestar Suporte Técnico Especializado.

2.3.12. Oferecer Treinamento técnico da Solução de Gerenciamento de vulnerabilidades

2.4 Requisitos de capacitação

2.4.1. Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.

2.4.1.1. O treinamento técnico da Solução de Gerenciamento de Vulnerabilidades será de, no mínimo, 40 horas, para turma de, no máximo, 8 alunos;

2.4.1.2. O treinamento, ou parte dele, poderá ser realizado no modelo telepresencial (online por videoconferência), em português, utilizando ferramenta própria disponibilizada pelo contratado (ex.: Microsoft Teams, Cisco Webex, Google Meet, etc.), desde que autorizado pelo Contratante;

2.4.1.3. O Contratante disponibilizará os computadores a serem utilizados pelos participantes do curso;

2.4.1.4. A CONTRATADA disponibilizará material didático oficial do curso em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento;

2.4.1.5. Caso não haja disponibilidade para realização nos modelos presencial ou telepresencial, a Contratada custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.

2.4.1.6. O treinamento deverá ser ministrado em português, por técnico certificado pelo fabricante da solução, e composto de aulas teóricas e práticas.

2.4.1.7. A CONTRATADA deverá confeccionar e disponibilizar aos participantes todo o material didático necessário ao treinamento, de todos os módulos que compõem a Solução.

2.4.1.8. A ementa e material utilizado no treinamento deverão ser enviados previamente ao Tribunal para avaliação e aprovação.

2.4.1.9. O treinamento deverá desenvolver o conhecimento e habilidades necessárias para fazer uso de todos os recursos disponíveis na Solução adquirida, incluindo, principalmente, a identificação dos Ativos de TI, o SCAN de Vulnerabilidades, Análise do SCAN, Avaliação de Riscos, Aplicação de Políticas, Compliance, dentre outras funcionalidades chaves da Solução.

2.4.1.10. Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso. As avaliações deverão ser preenchidas e assinadas pelos alunos e posteriormente entregues ao Tribunal para a assinatura do aceite da Ordem de Serviço do treinamento.

2.4.1.11. Caso o treinamento seja avaliado como insatisfatório pela maioria dos participantes da turma, o treinamento deverá ser refeito.

2.4.1.12. Será considerado insatisfatório o treinamento que obtiver maioria dos itens da avaliação de treinamento julgados como RUIM ou REGULAR, observadas todas as avaliações preenchidas.

2.4.1.13. O treinamento a ser refeito por ocasião de ter sido mal avaliado não pode gerar novas despesas para o CONTRATANTE.

2.4.1.14. Ao final do treinamento, cada participante deverá receber um certificado assinado pela CONTRATADA, contendo informações de data, carga horária, conteúdo ministrado, além do nome completo do instrutor, do aluno e da instituição que forneceu o curso, bem como o seu período.

2.4.1.15. A Contratada deverá fornecer certificado para cada aluno contendo identificação da instituição que forneceu o treinamento, nome do aluno, local do treinamento, período do treinamento, carga horária, nome do instrutor e conteúdo programático

2.5. Requisitos Suporte Técnico

2.5.1. A CONTRATADA deverá fornecer serviços de manutenção e suporte técnico pelo período de 60 (sessenta) meses, contados da data da assinatura do contrato de suporte técnico especializado, contemplando o suporte técnico para os sistemas e/ou appliances que compõem a Solução de Gerenciamento de Vulnerabilidades;

2.5.2. A CONTRATADA deverá prestar serviço de manutenção e suporte técnico destinado a:

2.5.2.1. Restabelecimento de serviços interrompidos ou degradados;

2.5.2.2. Solução de problemas de configuração e falhas técnicas nos serviços;

2.5.2.3. Esclarecimentos de dúvidas sobre configurações e utilização dos serviços;

2.5.2.4. Implementação de novas funcionalidades.

2.5.2.5. Entre outras situações correlatas às acima exemplificadas;

2.5.3. A CONTRATADA deverá atender as seguintes premissas:

2.5.3.1. Os serviços serão solicitados mediante a abertura de chamados a serem efetuados por técnicos do Tribunal, via chamada telefônica local ou gratuita, e-mail ou website, sem custos para a CONTRATANTE.

2.5.3.2. Não haverá limitação de quantidade de abertura de chamados para suporte.

2.5.3.3. O suporte deve estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nos 365 (trezentos e sessenta dias) do ano, sendo o Português Brasileiro o idioma de suporte técnico obrigatório.

2.5.3.4. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá à CONTRATADA fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços.

2.5.3.5. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.

2.5.3.6. O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.

2.5.4. Requisitos de Atendimento:

2.5.4.1. A CONTRATADA deverá realizar, mensalmente, procedimento de health check (check up) das configurações da(s) ferramenta(s) que façam parte da solução, propondo as melhorias necessárias através de relatórios, baseando-se nas boas práticas recomendadas pelo fabricante;

2.5.4.2. A CONTRATADA deve emitir, mensalmente, relatórios de vulnerabilidades e proposições de melhorias, no contexto da solução contratada, para avaliação do CONTRATANTE:

2.5.4.2.1. Procedimentos de correção e/ou contramedidas recomendadas pela equipe especializada da Contratada;

2.5.4.2.2. Orientações para o System Hardening dos serviços, servidores, elementos ativos e aplicações avaliados;

2.5.4.2.3. Sugestão para incremento da segurança e proteção do ambiente;

2.5.4.2.4. Os relatórios devem ser entregues em português, podendo os anexos técnicos possuírem dados em língua inglesa.

2.5.4.3. A CONTRATADA deve comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade, bem como a realização permanente de ações proativas voltadas ao incremento da segurança do parque computacional da JMU, a fim de mantê-lo estável, disponível e íntegro.

2.5.4.4. A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura, quando tais alterações envolver a solução ora contratada;

2.5.4.5. A CONTRATADA deverá realizar, no contexto da solução contratada, sob autorização e supervisão da CONTRATADA: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, resolução de problemas e implementação de segurança.

2.5.4.6. Os relatórios produzidos devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência de preferência do CONTRATANTE.

2.5.4.7. Não serão aceitos relatórios obtidos diretamente de ferramentas automatizadas utilizadas, sem a devida transcrição e contextualização adequada com o ambiente da JMU.

2.5.5. Dos prazos de atendimento:

2.5.5.1. A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados			
Severidade	Descrição	Tempo para primeiro contato após abertura do chamado	Tempo de resolução do chamado
Urgente	Serviço crítico parado em produção.	30 minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	Até 04 (quatro) hora

Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção.	120 minutos	Até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	Até 24 (vinte e quatro) horas

2.5.5.2. O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do suporte, através de telefone ou e-mail;

2.5.6. A CONTRATADA deve apresentar relatório de visita para cada solicitação de suporte on-site, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

2.5.7. O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do CONTRATANTE;

2.5.8. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados;

2.5.9. O descumprimento dos prazos de atendimento implicará na aplicação de glosas conforme tabela abaixo:

Tabela de aplicação de Glosas		
Severidade	Fórmula de cálculo da glosa	Limite da glosa
Urgente	HS x 0,5% * VFM	20% da VFM
Alta	HS x 0,4% * VFM	15% da VFM
Média	HS x 0,3% * VFM	10% da VFM
Baixa	HS x 0,2% * VFM	10% da VFM
Informações	HS x 0,1% * VFM	10% da VFM
HS = Horas totais que extrapolaram o limite de resolução dos chamados, no caso de hora quebrada, será apurado o percentual da hora descumprida.		
VFM = Valor da Fatura Mensal para pagamento do serviço de suporte.		
Em caso de descumprimento contumaz pela CONTRATADA nos prazos para atendimento do suporte técnico a fiscalização poderá adotar a aplicação de sanções: advertências, multas, suspensão temporária de participação em licitação e impedimento de contratar com a Administração e 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, na forma da lei 8.666, de 1993.		

2.5.10. A CONTRATADA deve emitir relatório mensal em arquivo eletrônico ou em sistema de consulta online, com informações dos chamados abertos e fechados no período;

2.5.11. O relatório deve possuir os seguintes parâmetros:

2.5.11.1. Quantidade de ocorrências (chamados) registradas no período;

2.5.11.2. Número do chamado registrado e nível de severidade;

2.5.11.3. Data e hora de abertura;

2.5.11.4. Data e hora de início e conclusão do atendimento;

2.5.11.5. Identificação do técnico que fez o registro do chamado;

2.5.11.6. Descrição do problema;

2.5.11.7. Descrição da solução;

2.5.12. Problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução, não deverão se encaixar nos prazos estabelecidos acima;

2.5.13. A CONTRATADA deverá, de acordo com o nível de criticidade, prover solução paliativa para atender os problemas de falhas (bugs), atualizações ou patches de correção que ainda não foram disponibilizadas pela fabricante, no prazo de 24 (vinte e quatro) horas, para restabelecer o ambiente do CONTRATANTE;

2.5.14. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias, sendo a CONTRATADA responsável pelos trâmites juntamente a fabricante da liberação das correções.

2.5.15. Nas manutenções que necessitem de intervenção para parada física ou reinicialização do equipamento, o CONTRATANTE deverá ser notificado previamente para que faça o agendamento da manutenção e aprovação;

2.5.16. As paradas de manutenção deverão acontecer fora do horário de expediente, de preferência após a 20 (vinte) horas devendo ser restabelecida antes das 8 (oito) horas da manhã do dia seguinte. Poderá ocorrer durante o dia da semana ou aos finais de semana, sem ônus para o CONTRATANTE;

2.5.16.1. Todo o procedimento de manutenção deverá ser documentado, explicando o passo a passo completo e fazendo registro das ocorrências incoerentes para subsidiar novas paradas que possam acontecer;

2.5.16.2. O relatório deverá ser assinado pelo fiscal técnico do contrato ou responsável pelo acompanhamento do serviço por parte do CONTRATANTE.

2.6. **Requisitos de segurança da informação**

2.6.1. O fornecedor deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do STM.

2.6.2. Deverá, ainda, manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto deste processo de contratação, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.

2.6.3. As informações a serem tratadas de forma sigilosa, restrita e confidencial são aquelas que, por sua natureza, são consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:

2.6.3.1. Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto serem divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo STM a tais documentos;

2.6.3.2. Resultados, parciais ou totais, sobre produtos gerados;

2.6.3.3. Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;

2.6.3.4. Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do STM e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros;

2.6.3.5. Documentos relativos à lista de usuários do STM e seus respectivos dados, armazenados sob qualquer forma;

2.6.3.6. Metodologias e ferramentas de serviços, desenvolvidas pelo STM;

2.6.3.7. Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do STM, sejam eles executados interna ou externamente;

2.6.3.8. . Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do STM, sejam elas residentes interna ou externamente;

2.6.3.9. Circulares e comunicações internas do STM;

2.6.3.10. Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo STM.

3. SOLUÇÕES DISPONÍVEIS NO MERCADO

Cenário 1 - Desenvolver solução interna de Gerenciamento de Vulnerabilidades: Tal alternativa necessita que a equipe de tecnologia da informação deste Tribunal desenvolva uma solução de hardware e software que realize os scans de vulnerabilidades, com relatórios, análise de riscos e compliance. Demandando bastante tempo, recursos humanos e investimento em qualificação da equipe em segurança da informação.

Cenário 2 - Utilização de Solução de software livre. Não foi encontrada solução que atenda aos requisitos presentes neste documento, no Portal do Software Público Brasileiro (http://softwarepublico.gov.br). As ferramentas gratuitas disponíveis para download e utilização são limitadas em funcionalidades, quantidade de scans realizados, relatórios gerados, tipos de ativos suportados e não possuem suporte técnico adequado, além disso, poucas englobam o processo de gerenciamento de vulnerabilidades, com análise de riscos e compliance, e os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas, tornando-as

incompatíveis com as necessidades do STM

Cenário 3 - Solução consolidada no mercado que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades baseada em nuvem (cloud computing) apresenta facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e módulo WAS), Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis, não é recomendável estarem armazenados em nuvem pública.

Cenário 4 - Solução consolidada no mercado que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseada em gerenciamento em rede local do tribunal (On premises). As soluções baseadas em gerenciamento em rede local (On premises) costumam apresentar um valor de aquisição menor do que a Cenário 3 (On cloud), pois os dados são gerenciados na própria infraestrutura da contratante. Apesar do Cenário 4 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis (como relatório de vulnerabilidades dos ativos de TIC do tribunal) pois estes dados serão armazenados na rede local do Tribunal e não em nuvem pública. Os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.sc) e Rapid7 (Nexpose e módulo AppSpider) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Outro ponto favorável do Cenário 4, é o fato de que, após o término do suporte, a SETIC continuará a ter acesso à ferramenta, embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

4. CONTRATAÇÕES SIMILARES REALIZADAS POR OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA

Órgão da Administração Pública	Contrato
Ministério Público MS	CONTRATO Nº 116/PGJ/2022
O TRIBUNAL DE CONTAS DE SANTA CATARINA – TCE/SC	CONTRATO Nº 36/2022 – TCE/SC
TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA	CONTRATO Nº 09/22-AQ
GOVERNO DO ESTADO DO PARÁ	CONTRATO Nº 024/2022

5. DETALHAMENTO DAS ALTERNATIVAS EXISTENTES

Requisitos	Itens da Solução	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?		X		
A solução encontra-se implantada em outro órgão ou entidade da Justiça Militar?				X
A Solução está disponível no Portal do Software Público Brasileiro?				X
A solução é um software livre ou público?				X
A solução é aderente às politicas, premissas e especificações técnicas definidas pelos padrões MNI?				X
A solução é aderente às regulamentações da ICP-Brasil?				X
A solução é aderente às premissas e especificações técnicas e funcionais do Moreq-Jus?				X

6. ESTIMATIVA DE PREÇO

A) Proposta 01 Empresa Fasthelp (2952954)

Grupo					
Item	Especificação	Unidade	Qtd. Total	Custo Unitário	Total
1	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Licença	2000	R$ 2.110,00	R$ 4.220.000,00
2	Treinamento técnico da Solução de Gerenciamento de Vulnerabilidades.	Pessoas	8	R$ 12.500,00	R$ 100.000,00

Valor Total	**R$** 4.320.000,00

B) Proposta 02 Emrpesa NTSEC (2952956)

Grupo					
Item	Especificação	Unidade	Qtd. Total	Custo Unitário	Total
1	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Licença	2000	R$ 1.980,00	R$ 3.960.000,00
2	Treinamento técnico da Solução de Gerenciamento de Vulnerabilidades.	Pessoas	8	R$ 15.000,00	R$ 120.000,00
Valor Total					**R$** 4.080.000,00

C) Proposta 03 Empresa GlobalSEc (2956717)

Grupo					
Item	Especificação	Unidade	Qtd. Total	Custo Unitário	Total
1	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Licença	2000	R$ 2.185,00	R$ 4.370.000,00
2	Treinamento técnico da Solução de Gerenciamento de Vulnerabilidades.	Pessoas	8	R$ 15.500,00	R$ 124.000,00
Valor Total					**R$** 4.494.000,00

C) Ata de Registro de Preços TRT 8 (2954943)

Grupo					
Item	Especificação	Unidade	Qtd. Total	Custo Unitário	Total
1	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Licença	2000	R$ 1.453,00	R$ 2.906.000,00
2	Treinamento técnico da Solução de Gerenciamento de Vulnerabilidades.	Pessoas	8	R$ 8.600,00	R$ 68.800,00
Valor Total					**R$ 2.974.800,00**

O Valor médio para a contratação é de R$ 3.967.200,00

7. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DAS SOLUÇÕES IDENTIFICADAS

Não há

8. ESCOLHA DA SOLUÇÃO

O cenário 1 fica prejudicado por não termos quadro de pessoal suficiente para este desenvolvimento, o cenário 2 como descrito acima não contempla todas as necessidades de verificação e proteção para garantir um mínimo de segurança além de demandarem uma maior sobrecarga de trabalho das equipes internas.

Os cenários 3 e 4 atendem aos requisitos da contratação, assim sendo foram pesquisadas soluções no mercado, as principais destacadas abaixo.

Solução 1: F-Secure Elements Vulnerability Management.

Solução 2: Qualys Vulnerability Management.

Solução 3: Rapid7 InsightVM.

Solução 4: Tenable: Tenable Security Center.

Portanto, é possível contratar por licitação própria, ou utilizando a Ata de Registro de Preços. O Tribunal Regional do Trabalho da 8ª Região realizou Pregão Eletrônico para contratação de Solução que auxilie na prevenção e limitação de ataques cibernéticos, através de gerenciamento de vulnerabilidade, que culminou na Ata de Registro de Preços Nº 5/2022, gerenciada pelo TRT da 8ª Região.

Considerando a economia e as vantagens de uma solução para todos os Tribunais, que gera sinergia e favorece a troca de informações, nivelando o conhecimento. Com a utilização desta ata teremos todas as vantagens do Cenário 4, pois baseia-se no gerenciamento da rede local do tribunal, apresentando ainda menor preço e realizando gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web, sem o armazenamento de dados sensíveis em nuvem pública.

Estando os preços da Ata de Registro de Preços do TRT8 dentro dos valores praticados pelo mercado, esta equipe recomenda a sua utilização.

9. DESCRIÇÃO DA SOLUÇÃO

Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.

10. ALINHAMENTO DA SOLUÇÃO

A solução se harmoniza com as necessidades do STM e não há conflitos com os requisitos tecnológicos existentes.

A Solução encontra-se alinhada com o Planejamento Estratégico Institucional

Objetivo: Fortalecer a governança e a segurança de dados e informações.

Estratégia: Compatibilizar a infraestrutura e as soluções de TIC às necessidades da JMU.

Iniciativa: Aperfeiçoar a gestão e a proteção de dados e informações.

11. BENEFÍCIOS ESPERADOS

11.1. Dentre os benefícios, destaca-se a redução de riscos e vulnerabilidades identificados de forma periódica e orientada à riscos.

11.2.Redução do risco de vazamento de informações da JMU, dos magistrados, servidores e jurisdicionados; garantia da continuidade do negócio; além da própria imagem institucional.

11.3.Uma solução em gerenciamento de vulnerabilidades permite a varredura de vulnerabilidades dos ativos de tecnologia da informação, de forma periódica e orientada a riscos, provendo relatórios detalhados e ações que tornam os ativos mais seguros e eficientes.

11.4.Além disso, oferece funcionalidades relacionadas ao processo de gerenciamento de vulnerabilidades, como gestão de baselines, compliance e atribuição de scores aos ativos escaneados.

12. RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA

Esta contratação se destina, fundamentalmente, a prevenir e limitar a extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseado em risco, dos ativos de Tecnologia da Informação, com análise contínua e adaptável de riscos e confiança, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações.

Foi utilizado o último levantamento realizado pela equipe de infraestrutura, a qual apontou 2500 endpoints. Para sessenta meses de contrato, e por ser um parque de estações mais homogêneo, não há a necessidade de licenciar todos os endpoints, desta forma, definimos o valor de 2.000 Endpoints.

13. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

Não há

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	**Integrante Demandante**	**Integrante Administrativo**
Márcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luis Gustavo Costa Reis**

VALIDAÇÃO DA ANÁLISE DE VIABILIDADE
IANNE CARVALHO BARROS **Diretor de Tecnologia da Informação**

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 22/11/2022, às 17:51 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIA - Apoio Especializado - Análise de Sistemas**, em 22/11/2022, às 18:21 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **INTEGRANTE ADMINISTRATIVO**, em 22/11/2022, às 18:39 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2952924** e o código CRC **1B3C8B88**.

2952924v34