ETP – Estudo Técnico Preliminar

AV – Análise de Viabilidade

1. IDENTIFICAÇÃO DO PROJETO

DP-1201 - Aquisição de Solução - Proteção de *Endpoint*

2. PROCESSO SEI

Processo SEI nº 0265066-66.2024.8.13.0000, DOD no evento 21190029.

3. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Equipe de Planejamento da Contratação			
Matrícula	**Nome**	**Área**	**Integrante demandante / técnico / administrativo / gestor**
00022921	Márcio Henrique Camargos d'Ávila	CESEC	Integrante demandante
00078055	Alan Carreiro Almeida	CESEC	Integrante técnico
00081513	Paulo César da Silva	CESEC	Integrante técnico

Tabela 1

4. FUNDAMENTO

4.1.A Importância da Segurança de *Endpoints* no TRIBUNAL

4.1.1. Hoje em dia, seja em um ambiente corporativo ou residencial, diversos dispositivos estão constantemente interconectados. Entre estes dispositivos, encontramos computadores, *notebooks*, servidores de rede, smartphones e tablets. Independentemente de sua natureza — móveis ou fixos, físicos ou virtuais — todos são classificados como ***endpoints***.

4.1.2. Traduzido literalmente, "*endpoint*" pode ser interpretado como "ponto de extremidade" ou "ponto final". Em termos simples, qualquer dispositivo conectado a uma rede é considerado um *endpoint*. Esse termo é amplamente utilizado na área de Tecnologia da Informação (TI), especialmente entre profissionais responsáveis pela gestão de redes corporativas.

4.1.3. Por terem capacidade de instalação e execução de aplicativos e outros códigos executáveis, manterem em execução e armazenados serviços e dados relevantes e estarem geralmente interligados à redes de dados corporativa e à internet, os *endpoints* são visados para invasão, fraude, obtenção de acessos indevidos, execução de códigos maliciosos, interceptação ou adulteração de tráfego de dados, exfiltração de dados sensíveis, entre outros tipos de ameaças e ataques.

4.1.4. Portanto, a proteção especializada, eficaz e eficiente destes dispositivos, com capacidades de prevenção, monitoramento, detecção e resposta a ações maliciosas, é componente essencial para a integridade e a segurança cibernética de um ambiente corporativo. Como ações maliciosas podem ocorrer a partir da exploração de alguma vulnerabilidade presente em qualquer *endpoint* de uma organização e, a partir desta exploração, possibilitar o alcance de alvos mais sensíveis e valiosos da organização, é essencial que a proteção dos *endpoints* seja a mais abrangente possível.

4.1.5. Além disso, é necessário que a proteção dos *endpoints* seja feita de forma integrada e coordenada com todo o ecossistema de segurança cibernética corporativo, incluindo as capacidades de monitoramento, detecção e resposta, gestão de vulnerabilidades, segurança de redes e proteção de dados.

4.2.Contexto e Necessidade de Atualização

4.2.1. O Tribunal de Justiça de Minas Gerais, assim como qualquer outra organização que faça uso de *endpoints* em seu cotidiano, está inserido em um cenário de ameaças cibernéticas cada vez mais sofisticadas e diversificadas. A solução de segurança de *endpoint* atualmente em uso, o **Symantec Endpoint Protection (SEP)**, não atende às demandas atuais do TRIBUNAL. Entre as principais lacunas de atendimento estão:

4.2.1.1. Falta de suporte a sistemas operacionais Linux: A solução atual não abrange servidores Linux, que fazem parte da infraestrutura central do TRIBUNAL.

4.2.1.2. Falta de suporte a dispositivos móveis: A solução atual não abrange dispositivos portáteis do TRIBUNAL, tais como tablets.

4.2.1.3. Integração limitada com a plataforma de monitoramento de segurança cibernética atualmente utilizada pelo TRIBUNAL: A solução atual não permite uma integração com a plataforma de monitoramento de segurança cibernética *Open XDR* da *Stellar Cyber*, instalada no TRIBUNAL, de forma a possibilitar o envio e execução de comandos administrativos no *endpoint* a partir da plataforma de monitoramento de segurança cibernética. Essa limitação afeta a capacidade de resposta a incidentes, comprometendo a eficácia da estratégia de segurança do TRIBUNAL.

4.2.1.4. Falta de serviços gerenciados, sustentação e suporte técnico da solução: Atualmente o TRIBUNAL não conta com um serviço gerenciado amplo e especializado para atuação continuada, nem remoto nem alocado nas dependências do TRIBUNAL, dependendo exclusivamente do suporte técnico básico do fabricante, que é insuficiente e não atende às necessidades operacionais do TRIBUNAL.

4.2.1.5. Desatualização tecnológica: De acordo com o Quadrante Mágico do Gartner, o Symantec SEP está cada vez mais distante dos líderes em soluções de proteção de *endpoint*, indicando que a solução atual não está alinhada com as melhores práticas e tecnologias do mercado.

4.3.Situação Contratual da Solução Atualmente em Uso

4.3.1. A solução atualmente em uso foi contratada em julho/2022 através do contrato CT 243-2022 com a TABTEC e tem vigência até 31/07/2026.

4.3.2. O contrato tem como objeto a subscrição (assinatura) de licenças do Symantec Endpoint Protection (SEP), para proteção de estações de trabalho, notebooks, workstations, servidores Windows e máquinas virtuais Windows, com garantia de atualização e suporte técnico do fabricante.

4.3.3. Está previsto no contrato a compatibilidade do SEP com os sistemas operacionais Windows 7 Professional, Windows 10 Pro e Windows 11 Pro.

4.3.4. Foram contratadas inicialmente 27.500 licenças, sendo que em julho de 2023, houve o acréscimo de 2.500 licenças no 1º Termo Aditivo (TA), totalizando 30.000 licenças.

4.3.5. Em julho/2024, houve a redução de 25% do quantitativo do contrato no 2º TA, totalizando 22.500 licenças.

4.3.6. O valor atualizado do contrato é de R$ 1.355.032,96.

5. ALINHAMENTO ESTRATÉGICO

5.1. Planejamento Estratégico Institucional – PEI

5.1.1. Macrodesafio: XII Fortalecimento da Estratégia de Tecnologias da Informação e Comunicação - TIC e de Proteção de Dados.

5.1.2. Iniciativa: 24. Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação.

5.2. Plano de Contratações Anual: Previsto no Plano de Contratações de 2025.

6. REQUISITOS DA SOLUÇÃO

6.1. Requisitos de negócio

6.1.1. Aspectos funcionais da Solução

6.1.1.1. Fornecimento de serviço gerenciado de segurança de *endpoints*, incluindo a atualização, manutenção e suporte técnico do fabricante.

6.1.1.1.1. A CONTRATADA deverá fornecer o serviço gerenciado de segurança de *endpoints* do TRIBUNAL, de forma a abranger computadores, servidores (Windows e Linux), dispositivos móveis (atualmente restritos a tablets), e estações virtuais com uma solução de proteção de *endpoint*.

6.1.1.1.2. A solução a ser utilizada no serviço gerenciado deverá ser integrada com a plataforma de monitoramento de segurança cibernética *Open XDR* da *Stellar Cyber*, instalada no TRIBUNAL, de forma a possibilitar o provimento da telemetria dos eventos que porventura ocorram com o *endpoint* para a plataforma de monitoramento instalada no TRIBUNAL, assim como possibilitar o envio e execução de comandos administrativos no *endpoint* a partir desta. Deve também suportar integrações com outras plataformas amplamente reconhecidas e abrangentes no mercado de monitoramento, detecção e resposta de segurança, SIEM e XDR, caso o TRIBUNAL venha futuramente adotar outra plataforma de monitoramento de segurança cibernética.

6.1.1.1.3. A solução a ser utilizada no serviço gerenciado deverá fornecer proteção contra ameaças avançadas:

a. Detecção e bloqueio em tempo real: Capacidade de identificar e neutralizar ameaças como *malwares*, *ransomwares*, *phishing*, *exploits* e ataques de dia zero imediatamente.

b. Análise comportamental: Conforme Termo de Referência, uso de técnicas avançadas para detectar atividades suspeitas, mesmo sem assinaturas conhecidas, através da análise do comportamento dos processos e aplicativos (UEBA).

6.1.1.1.4. A solução a ser utilizada no serviço gerenciado deverá fornecer monitoramento e detecção em tempo real:

a. Visibilidade contínua: Monitoramento em tempo real de todos os *endpoints*, com registros detalhados de atividades, processos e comportamentos.
b. Correlação de eventos: Capacidade de correlacionar eventos de segurança de diferentes *endpoints* para identificar padrões e atividades suspeitas.

6.1.1.1.5. A solução a ser utilizada no serviço gerenciado deverá ter resposta automatizada e manual a incidentes:

a. Resposta automatizada: Implementação de mecanismos automatizados para conter e mitigar ameaças rapidamente, incluindo isolamento de dispositivos, bloqueio de processos maliciosos e remoção de arquivos comprometidos.
b. Intervenção manual: Suporte para resposta manual, permitindo que equipes especializadas realizem investigações detalhadas e recomendem ações de mitigação.

6.1.1.1.6. A solução a ser utilizada no serviço gerenciado deverá ter gerenciamento centralizado e baseado em nuvem:

a. Console centralizado do próprio fabricante da solução: Plataforma de gerenciamento unificada, baseada em nuvem, para administração, configuração, monitoramento, centralização de eventos e geração de relatórios.

6.1.1.1.7. A solução a ser utilizada no serviço gerenciado deverá fazer análise de comportamento e inteligência de ameaças:

a. Inteligência Artificial (IA) e Machine Learning (ML): Aplicação de IA e ML para identificar comportamentos anômalos e prever possíveis ameaças e ataques, melhorando a detecção e resposta diante destas.
b. Feeds de Inteligência de Ameaças: Integração com fontes externas de inteligência para atualizar continuamente a base de conhecimento e melhorar a capacidade de resposta.

6.1.1.1.8. A solução a ser utilizada no serviço gerenciado deverá oferecer recursos eficientes e flexíveis para minimizar e limitar o consumo excessivo de processamento, memória, armazenamento e tráfego de rede, de forma a manter um uso racional e controlado de recursos dos *endpoints* e do ambiente corporativo de TIC.

6.1.1.1.9. A solução a ser utilizada no serviço gerenciado deverá ter atualizações automáticas e manutenção contínua:

a. Atualizações automáticas: Atualização contínua de definições de vírus, regras de segurança, mecanismos e patches de software para garantir eficácia e proteção constantes.
b. Manutenção proativa: Realização de manutenção regular para assegurar o desempenho eficiente da solução ao longo do tempo.
c. Permitir recursos flexíveis e eficientes de agendamento, segmentação e faseamento de atualizações e implantações em larga escala.

6.1.1.1.10. A solução a ser utilizada no serviço gerenciado deverá incluir relatórios detalhados, que possibilitem a geração de documentos abrangentes que registrem ameaças identificadas, medidas tomadas e o panorama geral da proteção.

6.1.1.1.11. A solução a ser utilizada no serviço gerenciado deverá ter prevenção proativa e análise de vulnerabilidades:

a. Identificação de vulnerabilidades: Capacidade de identificar vulnerabilidades nos *endpoints* e fornecer recomendações para correção antes que sejam exploradas.
b. Análise Preditiva: Uso de técnicas de análise preditiva para identificar tendências de ameaças e ajustar a estratégia de segurança da organização conforme necessário.

6.1.1.1.12. A solução a ser utilizada no serviço gerenciado deverá possuir certificações reconhecidas, como o *Common Criteria* (CC), que validam a segurança, confiabilidade e eficácia da solução de proteção de *endpoint*.

6.1.1.1.13. O serviço gerenciado deverá realizar verificações regulares na solução a ser utilizada, de forma a assegurar o alinhamento desta com normas de segurança e regulamentações aplicáveis.

6.1.2. Necessidade de capacitação

6.1.2.1. Não haverá capacitação, apenas *workshop* de apresentação da solução, conforme Termo de Referência.

6.1.3. Aspectos legais de conformidade

6.1.3.1. A solução a ser utilizada no serviço gerenciado deverá, no que couber, estar em conformidade com as normas nacionais e locais relacionados à segurança da informação e proteção de dados, incluindo a Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e a Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ, instituída pela Resolução CNJ nº 396/2021, seus protocolos e manuais.

6.1.3.2. A solução a ser utilizada no serviço gerenciado deverá, no que couber, estar alinhada com padrões internacionais de segurança, como NIST, ISO/IEC 27001, *CIS Controls* e *MITRE ATT&CK*.

6.1.4. Atualização, Manutenção e Suporte Técnico

6.1.4.1. A CONTRATADA deverá prestar serviços de atualização e suporte técnico, conforme descritos abaixo:

6.1.4.1.1. A CONTRATADA deverá prestar serviços de suporte técnico remoto e presencial.

6.1.4.1.2. Os serviços de atualização e suporte técnico englobarão resolução de problemas da solução de proteção de *endpoint*, resolução de dúvidas, atualizações dos softwares, sustentação da solução de proteção de *endpoint* no ambiente de nuvem e confecção de scripts para a Central de Atendimento do TRIBUNAL.

6.1.4.1.3. Os serviços de manutenção englobam a correção de erros do software, adaptação do mesmo a novas tecnologias, implementação de melhorias, prevenção de problemas futuros, otimização e ajustes do software.

6.1.4.1.4. A solução a ser utilizada no serviço gerenciado deverá receber atualizações automáticas e regulares de definições de vírus, regras de segurança e patches de software, com atualizações automáticas dos *endpoint*s, sem interrupção do serviço, exceto em situações específicas e excepcionais que exijam reinicialização ou procedimentos semelhantes.

6.1.4.1.5. A CONTRATADA deverá garantir o funcionamento contínuo da solução a ser utilizada no serviço gerenciado, com disponibilidade mínima de 99,9%, conforme níveis mínimos de serviços descritos no TERMO DE REFERÊNCIA, exceto em casos de manutenção programada ou eventos fora de seu controle.

6.1.4.1.6. A CONTRATADA deverá disponibilizar múltiplos canais de suporte, incluindo telefone 0800 ou local, e-mail e chat, para abertura de chamados no regime de 24 horas, 7 dias por semana, 365 dias por ano (24x7).

6.1.4.1.7. Os prazos de resolução dos chamados abertos e respectivos níveis mínimos de serviços serão estabelecidos no TERMO DE REFERÊNCIA.

6.1.4.1.8. O serviço de suporte presencial será prestado em horário comercial, ou seja, das 08:00 às 18:00, nas dependências do TRIBUNAL, com uma equipe dedicada e especializada.

6.1.4.1.9. O suporte presencial será prestado por uma equipe especializada, conhecedora do contexto e das necessidades do TRIBUNAL, conforme exigências descritas no item Equipe Técnica do TERMO DE REFERÊNCIA. A equipe presencial será formada por dois profissionais com perfil de técnicos especialistas e que além das atividades de suporte, serão o ponto de contato técnico com a equipe técnica do TJMG.

6.1.4.1.10. A CONTRATADA deverá prover, dentre outras coisas:

a. A emissão sob demanda de relatórios periódicos com histórico de ameaças detectadas, ações tomadas e status da proteção.
b. A realização de análises contínuas para garantir conformidade com regulamentações e normas de segurança aplicáveis.
c. A condução de análises preditivas para identificar tendências e padrões de ameaças atuais, auxiliando na melhoria da estratégia de mitigação de riscos.
d. A implementação de processos automatizados de detecção e mitigação de ameaças, de forma a reduzir a carga operacional e melhorar os tempos de resposta a incidentes.

6.1.4.1.11. A CONTRATADA estará sujeita a penalidades (glosas), estabelecidas no TERMO DE REFERÊNCIA, em caso de não conformidade com os acordos de nível de serviço (SLA) estabelecidos.

6.1.4.1.12. A CONTRATADA deverá garantir que a solução a ser utilizada no serviço gerenciado receba atualizações regulares de funcionalidades, alinhadas com as tendências do mercado e as necessidades do TRIBUNAL.

6.1.4.1.13. A CONTRATADA deverá coletar feedback do TRIBUNAL periodicamente e propor ajustes na solução para melhorar sua eficiência e adequação às necessidades operacionais.

6.1.5. Momento em que se pretende a entrega da solução

6.1.5.1. A estimativa é que a implantação de uma nova solução em todo o parque tecnológico do TJMG demande 8 meses e deve impreterivelmente ocorrer até 31/07/2026, quando o contrato atual se encerra.

6.1.6. Aspectos de segurança e privacidade

6.1.6.1. Segurança de Dados Confidenciais: A solução a ser utilizada no serviço gerenciado deverá possuir proteção de dados sensíveis com controles rigorosos, como criptografia, segmentação e controle de acesso.

6.1.7. Requisitos da Solução para estar em conformidade com os costumes, idiomas e o meio ambiente.

6.1.7.1. A solução a ser utilizada no serviço gerenciado deverá possuir interface e suporte técnico em língua portuguesa.

6.1.7.2. A solução a ser utilizada no serviço gerenciado deverá ser projetada para operar de maneira eficiente em termos de consumo de energia, contribuindo para a redução do impacto ambiental.

6.2.Requisitos tecnológicos

6.2.1. Arquitetura tecnológica

6.2.1.1. A solução a ser utilizada no serviço gerenciado deverá ser fornecida como SaaS - Software as a Service, com console de gerenciamento na nuvem da CONTRATADA ou fabricante da solução, de forma a permitir o gerenciamento centralizado de todos os agentes de segurança instalados nos *endpoint*s.

6.2.1.2. Estes agentes devem ser instalados localmente nos *endpoint*s do TRIBUNAL e deverão ser compatíveis com os seguintes sistemas operacionais:

a. Windows
   i. Windows 10 Pro;
   ii. Windows 11 Pro;
   iii. Windows Server 2016 e superior;
b. Linux
   i. Amazon Linux 2 e superior;
   ii. CentOS 8 e superior;
   iii. Debian 9.1 e superior;
   iv. Oracle Linux 7 e superior;
   v. Red Hat 7.4 e superior;
   vi. Ubuntu 18.04 e superior;

c. Dispositivos móveis
   i. Android 9 e superior;
   ii. iOS 16.0 e superior;
   iii. iPadOS 16.0 e superior.

6.2.2. Requisitos de Implantação da Solução

6.2.2.1. Responsabilidade pela Implantação

6.2.2.1.1. Planejamento do Projeto

a. A CONTRATADA deverá fornecer um cronograma detalhado com todas as etapas necessárias para a implantação da solução a ser utilizada no serviço gerenciado no TRIBUNAL.
b. Tal cronograma deverá ser elaborado e executado de forma a garantir que não haja interrupção dos serviços críticos e da proteção atualmente vigente.

6.2.2.1.2. Execução do Projeto

6.2.2.1.2.1. A execução do projeto de implantação será conduzida conforme o cronograma aprovado e abrangerá as seguintes etapas:

a. Levantamento de Requisitos: Identificar e documentar as necessidades e expectativas do TRIBUNAL.
b. Preparação do Ambiente: Garantir que a infraestrutura necessária esteja disponível e devidamente configurada.
c. Instalação e Configuração: Realizar a instalação e configuração dos agentes, garantindo a integração adequada com os sistemas existentes.
d. Testes de Funcionalidade: Testar todas as funcionalidades da solução para assegurar o pleno funcionamento.
e. Visão Geral: Conduzir um workshop detalhando todas as atividades realizadas durante a implantação, fornecendo uma explicação abrangente e técnica sobre a solução implementada. Não haverá capacitação da equipe interna.

6.2.2.1.3. Testes de Funcionalidade

6.2.2.1.3.1. Todas as atividades de implantação e configuração deverão ser testadas para garantir o pleno funcionamento da solução. Os testes incluirão, mas não se limitarão a:

a. Testes unitários de cada componente da solução.
b. Testes de integração entre os diferentes componentes e sistemas existentes.
c. Testes de desempenho para verificar a eficiência e eficácia da solução.
d. Testes de aceitação pelo TRIBUNAL para validar que a solução atende aos requisitos especificados.

6.2.2.1.4. Qualificação da Equipe

6.2.2.1.4.1. A implantação e configuração devem ser executadas por pessoal especializado, qualificado e com certificação oficial na solução. A equipe envolvida deve ter experiência comprovada em projetos semelhantes e estar

apta a solucionar possíveis problemas que possam surgir durante o processo de implantação.

6.2.2.1.5. Custos

6.2.2.1.5.1. Todas as despesas decorrentes do projeto de implantação, incluindo deslocamento, hospedagem e outros custos relacionados, serão suportadas integralmente pela CONTRATADA, sem ônus para o TRIBUNAL.

6.2.2.2. Processo de Desinstalação da Solução Atual

6.2.2.2.1. Desinstalação Completa

6.2.2.2.1.1. A CONTRATADA deverá, conforme Termo de Referência, realizar a desinstalação completa da solução de forma conjunta à instalação da solução a ser utilizada no serviço gerenciado, de forma a não prejudicar o nível de proteção vigente dos *endpoint*s.

6.2.2.2.1.2. Documentação do Processo

6.2.2.2.1.2.1. Todas as atividades realizadas durante a desinstalação deverão ser documentadas, incluindo:

a. Problemas encontrados.
b. Ações tomadas para resolvê-los.

6.2.2.2.1.2.2. A documentação deverá ser entregue ao TRIBUNAL logo que consolidada.

6.2.2.3. Implantação e Configuração da Nova Solução

6.2.2.3.1. Instalação dos Componentes

6.2.2.3.1.1. A CONTRATADA deverá implantar em sua última versão estável todos os componentes da solução a ser utilizada no serviço gerenciado.

6.2.2.3.2. Configuração Completa

6.2.2.3.2.1. A solução a ser utilizada no serviço gerenciado deverá ser configurada de acordo com as melhores práticas de segurança, incluindo:

a. Definição de políticas de segurança.
b. Calibração para adequação ao consumo racional e eficiente de recursos de TIC e à integração eficiente ao ambiente e infraestrutura tecnológica do TRIBUNAL.
c. Incorporação de regras, exceções e outras configurações necessárias à adequação às características e requisitos já existentes do ambiente e dos serviços de TIC do TRIBUNAL.
d. Configuração de dashboards, relatórios e alertas, em coordenação com o TRIBUNAL.

6.2.2.3.3. Customização e Distribuição dos Agentes

6.2.2.3.3.1. A CONTRATADA deverá, caso necessário e conforme o termo de referência, customizar os pacotes de instalação dos agentes de acordo com o tipo de *endpoint* e distribuí-los a todos os *endpoint*s do TRIBUNAL.

6.2.2.3.4. Integração com Ferramentas Existentes

6.2.2.3.4.1. A CONTRATADA deverá instruir a equipe técnica do TRIBUNAL com todas as informações necessárias para a integração da solução a ser utilizada

no serviço gerenciado com a plataforma de monitoramento de segurança cibernética *Open XDR da Stellar Cyber*, instalada no TRIBUNAL.

6.2.2.3.5. Documentação e Entrega

6.2.2.3.5.1. A CONTRATADA deverá entregar ao TRIBUNAL a documentação completa, incluindo:

a. Topologia da solução a ser utilizada no serviço gerenciado.
b. Relatório das atividades e configurações realizadas na instalação da solução a ser utilizada no serviço gerenciado.

6.2.2.3.6. Apresentação da Solução

6.2.2.3.6.1. A CONTRATADA, conforme Termo de Referência, deverá apresentar a solução a ser utilizada no serviço gerenciado configurada e implantada, demonstrando seu funcionamento e integração com a infraestrutura existente.

6.2.2.4. Garantia de Qualidade (*Quality Assurance*)

6.2.2.4.1. A implantação, conforme Termo de Referência, deverá incluir o serviço de *Quality Assurance* do fabricante da solução a ser utilizada no serviço gerenciado, assegurando a gestão de qualidade e a adoção das melhores práticas durante a implantação.

6.2.2.5. Aceitação

6.2.2.5.1. A CONTRATADA, conforme Termo de Referência, deverá realizar testes de aceitação em conjunto com o TRIBUNAL para garantir que a solução a ser utilizada no serviço gerenciado atenda aos requisitos técnicos e funcionais.

6.2.2.6. Condições Gerais e Responsabilidades

6.2.2.6.1. A CONTRATADA deverá garantir que todas as atividades sejam executadas com mínimo impacto nas operações do TRIBUNAL. Qualquer alteração no escopo ou no cronograma deve ser comunicada e aprovada previamente pelo TRIBUNAL.

6.2.3. Requisitos de Metodologia de Trabalho

6.2.3.1. A instalação e configuração dos agentes da solução a ser utilizada no serviço gerenciado, assim como a disponibilização da console de gerenciamento destes e das informações necessárias para integração desta solução à plataforma de monitoramento de segurança instalada no TRIBUNAL deverão ser realizadas pela CONTRATADA ou pelo fabricante desta, presencialmente, nas dependências do TRIBUNAL e com apoio da equipe remota.

6.2.3.2. A implantação deverá ser conduzida por profissionais certificados e qualificados, capazes de customizar as ferramentas conforme as necessidades do TRIBUNAL, seguindo a orientação profissional do fabricante da solução a ser utilizada no serviço gerenciado nas atividades de elaboração do projeto e validação da configuração durante a implantação.

6.2.3.3. A implantação da solução a ser utilizada no serviço gerenciado deverá ser conduzida de forma a garantir uma transição segura e controlada, incluindo a remoção completa e segura da solução de proteção de *endpoint* atual, assegurando que nenhum resíduo comprometa o desempenho ou a segurança do ambiente e nenhuma desinstalação seja

desacompanhada da imediata instalação da solução a ser utilizada no serviço gerenciado.

6.2.3.4. Para cada atividade, a CONTRATADA deverá elaborar e apresentar um plano de trabalho detalhado, alinhado às diretrizes e especificações estabelecidas no TERMO DE REFERÊNCIA, contendo:

6.2.3.4.1. Implantação das novas licenças e remoção da solução atual.

6.2.3.4.2. Suporte técnico e operação da solução a ser utilizada no serviço gerenciado, incluindo suporte aos usuários, ambos de forma remota.

6.2.3.4.3. Suporte com profissional dedicado nas dependências do TRIBUNAL.

6.2.3.5. Ao final da atividade, o TRIBUNAL deverá validar a conclusão dos trabalhos e emitir um aceite para que o serviço avance para a próxima atividade.

6.2.4. Requisitos da Gestão Contratual

6.2.4.1. Conforme o TERMO DE REFERÊNCIA, a contratada deverá disponibilizar profissionais qualificados, preferencialmente de forma remota, com expertise nas áreas de *Technical Account Management* (TAM) e *Customer Success* (CS) que serão responsáveis pela gestão do contrato, garantindo a excelência operacional e o alinhamento estratégico com os objetivos estabelecidos, em especial para:

6.2.4.1.1. Auxiliar na implementação da solução de proteção de *endpoint*, garantindo alinhamento com os objetivos do cliente.

6.2.4.1.2. Realizar análises proativas e recomendações para otimizar o uso da solução.

6.2.4.1.3. Acompanhar o suporte técnico especializado em situações críticas ou de alta complexidade.

6.2.4.1.4. Acompanhar e assegurar a adoção efetiva da solução pelo cliente.

6.2.4.1.5. Realizar reuniões periódicas para avaliar indicadores de desempenho (KPIs) e o cumprimento dos níveis de serviço (*SLAs*).

6.2.4.1.6. Desenvolver estratégias para maximizar o retorno sobre o investimento (ROI) da solução.

6.2.4.1.7. Realizar workshops, detalhando todas as atividades realizadas durante a implantação do projeto e fornecendo uma explicação abrangente e técnica sobre a solução.

6.2.4.1.8. Disponibilizar documentação técnica e melhores práticas.

6.2.4.1.9. Servir como ponto de contato único para alinhamento técnico e resolução de problemas.

6.2.4.1.10. Coordenar com outras equipes e ferramentas de segurança do cliente, assegurando integração eficaz.

6.2.4.1.11. Manter comunicação constante para alinhamento estratégico e técnico entre cliente e fornecedor.

6.2.4.1.12. Supervisionar o contrato durante toda a sua vigência, garantindo o cumprimento das cláusulas acordadas.

6.2.4.1.13. Gerenciar aspectos financeiros e orçamentários do contrato, incluindo custos, pagamentos e planejamento de renovações.

6.2.4.1.14. Relatar periodicamente o status contratual e financeiro ao cliente, promovendo transparência e alinhamento.

6.2.5. Perfis dos profissionais da CONTRATADA necessários à prestação dos serviços

6.2.5.1. Para assegurar a qualidade e a eficácia dos serviços, conforme o TERMO DE REFERÊNCIA, a CONTRATADA deverá comprovar, por meio de documentação hábil, a existência de profissionais devidamente qualificados e tecnicamente capacitados em sua equipe de atendimento e sustentação.

6.2.5.2. Os perfis profissionais deverão ser detalhadamente descritos no TERMO DE REFERÊNCIA, incluindo suas respectivas certificações e qualificações.

6.2.5.2.1. Profissionais de Implantação

a. Certificações reconhecidas pelo fabricante da solução de proteção de *endpoint*.
b. Habilidades e conhecimentos específicos comprovados.

6.2.5.2.2. Profissionais de Sustentação e Gestão Contratual da Solução (Presencial e Remoto)

a. Certificações reconhecidas pelo fabricante da solução de proteção de *endpoint*.
b. Habilidades e conhecimentos específicos comprovados.

6.2.5.3. As certificações deverão ser reconhecidas pelo fabricante da solução de proteção de *endpoint* ou possuir uma certificação equivalente, com especialidade comprovada.

6.2.5.4. Não haverá custos adicionais para o TRIBUNAL relacionados a essas certificações.

6.2.5.5. As certificações serão solicitadas e verificadas durante a reunião de *kick-off*, conforme TERMO DE REFERÊNCIA.

6.2.6. Aspectos de Segurança e Privacidade:

6.2.6.1. Proteção Multicamadas: A solução a ser utilizada no serviço gerenciado deverá fornecer uma proteção robusta contra ameaças cibernéticas, incluindo vírus, malware, ransomware, phishing e outras ameaças emergentes. A proteção deve ser proativa e capaz de detectar e neutralizar ameaças em tempo real.

6.2.6.2. Privacidade de Dados: A solução a ser utilizada no serviço gerenciado deverá garantir a privacidade dos dados do TRIBUNAL, devendo possuir recursos de criptografia para proteção de dados sensíveis.

6.2.6.3. Autenticação e Controle de Acesso: adoção de métodos de autenticação robustos, como autenticação multifator (MFA), para garantir que apenas usuários autorizados possam acessar e gerenciar a solução.

7. ESTIMATIVAS DAS QUANTIDADES

7.1. A solução atualmente em uso foi contratada em julho/2022 através do contrato CT 243-2022 com a TABTEC e tem vigência até 31/07/2026.

7.2. O contrato tem como objeto a subscrição (assinatura) de licenças do Symantec Endpoint Protection, para proteção de estações de trabalho, notebooks, workstations, servidores Windows e máquinas virtuais Windows, com garantia de atualização e suporte técnico já englobados os serviços de atualização e suporte técnico do fabricante.

7.3. Está previsto no contrato a compatibilidade do SEP com os sistemas operacionais Windows 7 Professional, Windows 10 Pro e Windows 11 Pro.

7.4. Foram contratadas inicialmente 27.500 licenças, sendo que em julho de 2023, houve o acréscimo de 2.500 licenças no 1º TA, totalizando 30.000 licenças.

7.5. A solução a ser utilizada no serviço gerenciado deve oferecer serviço gerenciado de proteção de *endpoint*s para até 43.500 dispositivos, considerando a infraestrutura tecnológica atual e a projeção de crescimento. As licenças e seus quantitativos serão divididos em categorias: servidores Linux, servidores Windows e dispositivos móveis.

7.6. Estimativa da demanda:

Item	Descrição	Unidade	Quantidade
1	Serviço Gerenciado de Segurança de Endpoint	Dispositivo	43.500
2	Serviço de implantação da solução no TRIBUNAL	Serviço	1

Tabela 2

7.7. Quantitativos atuais:

Dispositivo	Quantitativo
Estações de trabalho Windows (desktops, notebooks e workstations)	35.600
Estações de trabalho Windows (virtualizadas)	4.000
Servidores Windows	400
Servidores Linux	1.200
Dispositivos Móveis (tablets Android)	40
TOTAL	**41.240**

Tabela 3 - Referência maio/2025

7.7.1. Acrescido ao quantitativo total uma margem de segurança de 3,5% mais uma estimativa de crescimento anual de 3,5%, chegamos ao quantitativo ao final de 36 meses de 43.261. Arredondando este valor ao meio milhar, tem-se 43.500 endpoints.

8. LEVANTAMENTO DE MERCADO

8.1. Identificação das Soluções

8.1.1. Contratação de Serviço Gerenciado de Segurança de Endpoint (Solução Única)

8.1.1.1. Foi levantado no mercado a possibilidade de contratação de um serviço gerenciado de segurança de *endpoint*, em vez de contratação direta de subscrições de antivírus, que é o cenário atual.

8.1.1.2. Esse serviço a ser prestado pela CONTRATADA, seria responsável pela segurança cibernética de todos os *endpoint*s do TRIBUNAL, contemplando os licenciamentos dos softwares necessários e suas respectivas atualizações, assim como os serviços para a implantação da solução a ser utilizada no serviço gerenciado e o respectivo suporte técnico (que inclui resolução de problemas, resolução de dúvidas e o monitoramento constante dos *endpoint*s com atuação preventiva e corretiva de ameaças e incidentes).

8.1.1.3. A presente possibilidade envolveria uma mudança de paradigma, pois estaria sendo contratado um serviço que seria responsável pela segurança de todos os *endpoint*s do TRIBUNAL. Esse serviço englobaria um gerenciamento centralizado na nuvem da CONTRATADA ou do fabricante da solução, possibilitando um monitoramento constante do parque tecnológico do TRIBUNAL, permitindo uma atuação assertiva e mais rápida no combate às ameaças apresentadas, protegendo os sistemas e dados do TRIBUNAL.

8.1.1.4. Também seria exigido que a solução a ser utilizada no serviço gerenciado seja integrada com a plataforma de monitoramento de segurança cibernética *Open XDR* da *Stellar Cyber*, instalada no TRIBUNAL, de forma a possibilitar o provimento da telemetria dos eventos que porventura ocorram com o *endpoint* para a plataforma de monitoramento de segurança cibernética, assim como o envio e execução de comandos administrativos no *endpoint* a partir desta.

8.1.1.5. Por fim, além dos pontos citados acima seria exigido que a CONTRATADA utilize uma solução de proteção de *endpoint* mais robusta que utiliza tecnologias modernas, como inteligência artificial, machine learning e análise comportamental, para detecção e mitigação de ameaças avançadas e que seja instalada e posta em funcionamento contínuo em todos os *endpoint*s do TRIBUNAL (computadores, servidores, notebooks, dispositivos móveis, nos sistemas operacionais Windows, Linux, Android, iOS e iPadOS).

8.1.2. Soluções consideradas inviáveis

8.1.2.1. Continuidade da solução Symantec Endpoint Protection (SEP)

8.1.2.1.1. Limitações:

a. Falta de suporte a sistemas operacionais Linux: Não abrange servidores Linux.
b. Falta de suporte a dispositivos móveis: Não abrange dispositivos móveis.
c. Integração limitada com *Stellar Cyber* (*Open XDR*): Não permite integração ampla com a plataforma de monitoramento, limitando a visibilidade e a capacidade de resposta a incidentes.
d. Falta de serviços gerenciados de sustentação e operação e Suporte Técnico Especializado limitado: Dependência exclusiva do suporte básico do fabricante, que é insuficiente.
e. Desatualização Tecnológica: Classificação distante dos líderes em soluções de proteção de *endpoint* pelo Quadrante Mágico do Gartner de 2023.

8.1.2.1.2. Diante destas limitações, recomenda-se descartar quaisquer alternativas fundamentadas na solução SEP.

8.1.2.2. Contratação de subscrições de nova solução de proteção de endpoints e de serviços especializados de sustentação e operação

8.1.2.2.1. A contratação de subscrições como item de objeto separado dos serviços correlatos ainda é corrente no mercado, mas o modelo traz diversas limitações e dificuldades em relação a um modelo de serviços gerenciados de segurança (MSS) que engloba solução e serviços, a saber:

a. A subscrição é um modelo de mercado pago no início de cada ciclo, em geral anual, e na quantidade total de licenças (dispositivos) previstas, dificultando a remuneração proporcional à ativação gradativa (transição) ou à variação de licenças ativas, que são a situação presente, em que se objetiva a substituição da solução atual e a implantação e expansão de uma nova solução em etapas.

b. O licenciamento tem foco no produto e não na entrega e na eficácia e efetividade dos resultados esperados e, por ser tipicamente no início do ciclo, inviabiliza uma dinâmica mensal de apuração de níveis de serviço relativas a suporte técnico e outros aspectos inerentes, nem a consequente aplicação mensal de glosas quando há problemas ou inconformidades.

8.1.2.3. Diante destas limitações, recomenda-se descartar a contratação de subscrições de licenças, dissociada dos respectivos serviços de sustentação e operação.

8.1.3. Conclusão:

8.1.3.1. O TRIBUNAL necessita de uma nova solução de proteção de *endpoint* que ofereça:

8.1.3.1.1. Implantação e gestão contínua de segurança de *endpoint*.

8.1.3.1.2. Serviços gerenciados de sustentação, incluindo administração, operação e suporte técnico especializado e proativo.

8.1.3.1.3. Cobertura para servidores Linux e dispositivos móveis.

8.1.3.1.4. Integração ampla com a plataforma de monitoramento atual do TRIBUNAL, *Stellar Cyber* (*Open XDR*).

8.2. Identificação dos fabricantes e fornecedores

8.2.1. Os critérios principais adotados para a prospecção de prováveis fornecedores foram:

8.2.1.1. Identificar fabricantes de soluções de proteção de endpoint líderes de mercado, tomando como base o Quadrante Mágico de Plataformas de Proteção de Endpoint mais recente disponível do Gartner[1]: CrowdStrike, Microsoft, SentinelOne, Palo Alto, Sophos. O Gartner ainda enumera fabricantes relevantes nos quadrantes desafiante, visionário e de nicho, conforme figura a seguir.

[1] Gartner. “Magic Quadrant for Endpoint Protection Platforms”, 23/09/2024, documento ID G00808300, por Evgeny Mirolyubov, Franz Hinner, Deepak Mishra, Satarupa Patnaik, Chris Silva.

8.2.1.2. Identificar fabricantes de soluções Endpoint Security listados com integração nativa com a solução de monitoramento, detecção e resposta atualmente adotada pelo TJMG, Stellar Cyber Open XDR, tomando como base a lista de conectores homologados no site do fabricante Stellar Cyber para Endpoint Security para as integrações de Coleta e Resposta[2]: CrowdStrike, Cybereason, Cynet, Deep Inspect, Microsoft, SentinelOne, SonicWall, Sophos, VMware Carbon Black, WithSecure Elements. Outros fornecedores de soluções constam listados apenas com capacidade de coleta, ou apenas de resposta.

8.2.1.3. Identificar eventuais fornecedores e fabricantes que tenham presença relevante no mercado brasileiro no segmento de soluções de proteção de endpoint.

[2] Stellar Cyber. "Connectors and Integrations Summary", disponível em https://docs.stellarcyber.ai/5.4.x/Configure/Connectors/4-Connectors-Integrations.htm; e "Connector Types & Functions", Endpoint Security, Collect + Respond, disponível em https://docs.stellarcyber.ai/5.4.x/Configure/Connectors/1-Connectors-List.htm.

8.2.2. Para validar a contratação pretendida e obter cotações atualizadas, foram feitas consultas com os possíveis fornecedores abaixo:

	EMPRESA	FABRICANTE	DATA DA SOLICITAÇÃO	DATA DA RESPOSTA	OBSERVAÇÕES
1	Under Protection	Fortinet	29/05/2025	10/06/2025	Enviou proposta.
2	Disruptec	CrowdStrike	29/05/2025	-	Não apresentou proposta.
3	ISH	Sophos		16/06/2025	Enviou proposta.
4	Future	Sophos	29/05/2025	03/06/2025	Enviou proposta.
5	Shield Security	-	29/05/2025	-	Não apresentou proposta.
6	Microhard	Kaspersky	29/05/2025	25/06/2025	Não apresentou proposta.
7	Welt Solutions	-	29/05/2025	-	Não apresentou proposta.
8	Trend Micro (Tripla)	Trend Micro	29/05/2025	-	Não apresentou proposta.
9	TLM	SentinelOne	29/05/2025	-	Não apresentou proposta.
10	Brasoftware	Microsoft	29/05/2025	-	Não apresentou proposta.
11	BHF	Microsoft	29/05/2025	-	Não apresentou proposta.
12	VSP Solutions	Fortinet	29/05/2025	06/06/2025	A empresa informou que VSP Solutions e Under Protection são parceiras neste projeto e que a proposta seria pela Under Protection.
13	Checkpoint	Checkpoint	09/06/2025	-	Não apresentou proposta.

Tabela 4 - Referência junho/2025

9. ESTIMATIVA DO VALOR

Solução Única: CONTRATAÇÃO DE NOVA SOLUÇÃO SERVIÇO GERENCIADO DE SEGURANÇA DE ENDPOINT

Os custos estimados foram mensurados através de cotações com fornecedores de soluções que atendem aos requisitos apresentados.

De todos os fornecedores pesquisados, apenas 3 apresentaram propostas (ISH, Under Protection e Future). Considerando os requisitos necessários definidos neste estudo, a solução proposta pelo fornecedor Under Protection atualmente não possui conector homologado pela solução Stella Cyber, razão pela qual foi descartada.

SOLUÇÃO 1	ISH - 16/06/2025		Future - 03/06/2025	
Item	**Quant.**	**Unitário**	**Quant.**	**Unitário**
1 - Serviço gerenciado de segurança de endpoint de natureza continuada, estimados para até 43.500 dispositivos em 36 meses	36	R$ 707.697,550	36	R$ 627.948,39
2 - Serviço de implantação da solução	1	R$ 321.557,94	1	R$ 126.000,00
3 - Serviço técnico especializado de customização e apoio na solução, sob demanda, de natureza continuada, de até 600 horas por ano	1800	-	1800	R$ 545,45
	TOTAL (R$)	R$ 25.798.669,74	**TOTAL (R$)**	R$ 23.713.960,22

Tabela 5

Dado os custos apresentados, juntamente com a conhecida competitividade do mercado de segurança de endpoint, trabalharemos como estimativa de valor o menor custo apresentado em proposta (R$ 23.713.960,22).

10. DESCRIÇÃO E JUSTIFICATIVA DA SOLUÇÃO DE TIC A SER CONTRATADA

10.1. A solução recomendada a ser contratada é:

10.1.1. Contratação de serviço gerenciado de segurança de *endpoint*, abrangendo:

a. Fornecimento de 43.500 subscrições para licenciamento de uma solução de proteção de *endpoint*, com plataforma de gerenciamento (configuração e monitoramento) unificada, baseada em nuvem da CONTRATADA ou do fabricante da solução e agentes instalados localmente nos *endpoint*s, incluindo serviços de atualização e suporte técnico avançado do fabricante.

b. Serviços de sustentação, incluindo administração, operação, monitoramento, e suporte técnico da solução, sendo remoto na modalidade 24x7 e presencial, nas dependências do TRIBUNAL na Capital, em horário comercial.

10.1.2. Serviços de implantação da solução no TRIBUNAL, abrangendo a desinstalação da solução atual e a instalação e configuração da solução a ser utilizada no serviço gerenciado.

10.1.3. Customização da solução a ser utilizada no serviço gerenciado, por meio da prestação de até 1800 horas, conforme necessidade do TRIBUNAL.

10.2. Os benefícios da adoção desta Solução estão descritos no item 8.1 acima.

11.JUSTIFICAR O PARCELAMENTO OU NÃO DA SOLUÇÃO

11.1. A contratação de um serviço gerenciado de segurança de *endpoint* para substituir a solução atual deve ser realizada de forma estratégica, priorizando a integração, a eficiência operacional e a redução de riscos. Optar por um único fornecedor para a solução traz uma série de vantagens significativas, especialmente no que diz respeito à integração harmoniosa de todos os componentes do sistema. Quando diferentes empresas são contratadas para fornecer partes distintas da solução, podem surgir inconsistências e complicações na integração, o que pode comprometer o desempenho geral do sistema.

11.2. Além disso, a gestão de múltiplos contratos exige um maior dispêndio de recursos administrativos, aumentando não apenas a carga de trabalho, mas também os custos associados à fiscalização e à coordenação. Em situações de problemas técnicos ou falhas, a existência de vários fornecedores pode resultar em um jogo de "empurra-empurra", dificultando a identificação e a resolução rápida das questões. Isso pode levar a custos adicionais e a atrasos significativos, impactando negativamente a operação.

11.3. A comunicação e a coordenação entre várias empresas também podem se tornar complexas e arriscadas, especialmente quando os fornecedores possuem abordagens e culturas organizacionais distintas. Essas diferenças podem gerar conflitos e atrasos, comprometendo a eficiência do projeto. Em situações de emergência, onde uma resposta rápida e coordenada é crucial, a presença de múltiplos fornecedores pode dificultar a tomada de decisões e a adoção bem-sucedida de soluções, colocando em risco a continuidade das operações.

11.4. Ao contratar uma única empresa, é possível garantir uma transição mais suave e eficiente, sem interrupções ou conflitos entre fornecedores. A consistência no suporte técnico é outro fator crítico: um único fornecedor pode assegurar que as operações sejam contínuas e sem falhas, enquanto múltiplos fornecedores podem levar a inconsistências no suporte e na operação.

11.5. Ter profissionais dedicados da mesma empresa que vai prestar o serviço de suporte facilita a comunicação e a resolução de problemas, evitando confusões e atrasos que podem surgir quando há vários pontos de contato.

11.6. Em resumo, a contratação de uma única empresa para a prestação do serviço gerenciado de segurança de *endpoint* não apenas simplifica a gestão do projeto, mas também reduz riscos, custos e potenciais complicações, garantindo uma operação mais eficiente e segura.

12.DEMONSTRATIVOS DOS RESULTADOS PRETENDIDOS

12.1. A contratação de um serviço gerenciado de segurança de *endpoint*s trará benefícios significativos para o TRIBUNAL em termos de economicidade, eficiência operacional, segurança cibernética e aproveitamento de recursos humanos, materiais e financeiros. Abaixo, são detalhados os resultados esperados:

12.1.1. Economicidade e otimização de recursos financeiros:

a. Redução de custos com incidentes cibernéticos: A solução a ser utilizada no serviço gerenciado reduzirá os custos associados a possíveis incidentes de segurança, como vazamentos ou sequestro de dados, paralisação de sistemas e recuperação de infraestrutura, que podem gerar perdas financeiras e danos à reputação.

b. Escalabilidade eficiente: A adoção de um modelo baseado em serviço permitirá o TRIBUNAL desembolsar apenas pelos recursos que utilizaram o serviço, evitando desperdícios e garantindo que o crescimento da demanda por parte do TRIBUNAL seja acompanhado de forma econômica.

12.1.2. Melhor aproveitamento dos recursos humanos:

a. Redução da carga operacional: Com a automação de processos de detecção e resposta a ameaças, a equipe de TI poderá focar em atividades estratégicas, em vez de tarefas repetitivas de monitoramento e correção de incidentes.
b. Suporte técnico especializado: O monitoramento contínuo 24x7 e a presença de profissionais dedicados no TRIBUNAL garantirão respostas rápidas a incidentes, minimizando o tempo de inatividade e aumentando a produtividade das equipes.

12.1.3. Melhoria da qualidade dos serviços:

a. Proteção avançada contra ameaças: A solução a ser utilizada no serviço gerenciado proporcionará uma proteção mais robusta contra ameaças cibernéticas avançadas, incluindo malwares desconhecidos e ataques personalizados, garantindo a continuidade operacional e a integridade dos dados do TRIBUNAL.
b. Cobertura completa do parque tecnológico: Com suporte para computadores, notebooks, dispositivos móveis e servidores Windows e Linux, a solução eliminará lacunas de segurança, protegendo toda a infraestrutura tecnológica do TRIBUNAL.
c. Integração com *Stellar Cyber* (*Open XDR*): A integração integral com a plataforma de monitoramento de segurança cibernética permitirá uma visão mais ampla e atual das ameaças, juntamente com a possibilidade de uma orquestração unificada de respostas a tais ameaças.

12.1.4. Benefícios diretos esperados:

a. Conformidade com Normas de Segurança: O serviço garantirá que o TRIBUNAL esteja em conformidade com as regulamentações de segurança cibernética.
b. Resiliência a ataques cibernéticos: A capacidade de detectar e neutralizar ataques avançados reduzirá o risco de paralisação dos serviços judiciais, garantindo a continuidade das operações do TRIBUNAL.
c. Transição suave e sem conflitos: A desinstalação completa da solução de proteção atualmente utilizada (Symantec Endpoint Protection) e a implantação por ondas da solução a ser utilizada no serviço gerenciado garantirão uma transição eficiente, minimizando riscos de interrupções na proteção.

12.1.5. Mensuração dos resultados:

a. Redução no número de incidentes cibernéticos: Medição da diminuição de ataques bem-sucedidos e tempo médio de resposta a incidentes.
b. Cobertura de *endpoint*s protegidos: Percentual de servidores e dispositivos protegidos, incluindo Windows e Linux.
c. Satisfação da equipe de TI: Avaliação da eficácia da capacitação e da autonomia da equipe no gerenciamento da solução.
d. Conformidade com normas: Verificação do cumprimento das regulamentações de segurança cibernética.

13.PROVIDÊNCIAS

13.1. O contrato atual será gradualmente reduzido, conforme autorizado na reunião do CTIC, e rescindido após a conclusão da desinstalação do antivírus.

13.2. O serviço será executado nas dependências da CONTRATADA, com a alocação inicial de dois profissionais nas dependências do TRIBUNAL. Portanto, não será necessária a adequação no ambiente de TIC do TRIBUNAL.

13.3. Será necessário disponibilizar um ponto de trabalho para cada profissional presencial dedicado da CONTRATADA nas dependências do TRIBUNAL na Capital.

13.4. Além disso, deverá ser reservada a data e o local para o workshop de apresentação e transferência de conhecimento quando este for realizado.

14.CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

14.1. A contratação de uma solução de Serviço Gerenciado de Segurança de Endpoint está ligada ao contrato de MSS vigente atualmente no TRIBUNAL, pois ambos visam proteger os ativos de TI do TRIBUNAL. Para garantir uma proteção eficaz, é essencial planejar a integração entre o MSS e a solução a ser utilizada no serviço gerenciado a ser contratado.

14.2. O CONTRATO Nº 267/2024 com a FUTURE TECHNOLOGIES INFORMÁTICA LTDA. já oferece serviços de segurança cibernética (MSS), e a nova contratação visa complementar esses serviços.

15.IMPACTOS AMBIENTAIS

15.1. Redução do descarte de hardware: Um computador protegido por uma solução de proteção de *endpoint* tem menos probabilidade de ser infectado por malwares que podem danificar o sistema. Isso significa que o hardware pode ter uma vida útil maior, reduzindo a necessidade de descarte e, consequentemente, a produção de lixo eletrônico.

15.2. Economia de energia: Sistemas infectados geralmente operam de forma menos eficiente, consumindo mais energia. Ao manter o computador livre de ameaças cibernéticas e funcionando de maneira otimizada, a economia de energia pode ser significativa.

15.3. Menor demanda por novos equipamentos: Computadores que precisam ser substituídos com menos frequência devido a falhas causadas por ameaças cibernéticas contribuem para uma menor demanda por novos equipamentos. Isso ajuda a reduzir a extração de recursos naturais e a emissão de carbono associada à fabricação e transporte de novos dispositivos.

15.4. Proteção de dados: Com uma proteção eficiente, dados importantes e documentos digitais são protegidos contra-ataques cibernéticos, evitando a necessidade de processos adicionais de recuperação ou retrabalho que demandam energia e recursos.

16.POSICIONAMENTO CONCLUSIVO

16.1. Fica claro que a contratação da uma nova solução de proteção *endpoint* é não apenas viável, mas também essencial para atender às necessidades crescentes de segurança cibernética do TRIBUNAL.

16.2. Com base nos elementos apresentados neste documento, a contratação de um serviço gerenciado de segurança de *endpoint* que forneça tal solução é viável e necessário para o atendimento das necessidades de segurança cibernética do TJMG.

16.3. A solução a ser utilizada no serviço gerenciado superará as limitações da solução atual, proporcionando uma plataforma de segurança mais robusta, escalável e eficaz, além de garantir a conformidade com as regulamentações de segurança cibernética.

17. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

17.1. Recursos Materiais e Humanos

17.1.1. Recursos Materiais Necessários

a. Dispositivos *endpoint* para instalação e execução da solução;
b. Infraestrutura de rede adequada para suportar a implantação da nova solução;
c. Recursos de backup e recuperação para garantir a continuidade dos serviços durante a transição.

18. ESTRATÉGIA DE CONTINUIDADE DO FORNECIMENTO DA SOLUÇÃO DE TIC

18.1. Em caso de falência ou má **prestação** de serviços pela CONTRATADA, o TRIBUNAL deve adotar medidas para garantir a continuidade da proteção. As estratégias incluem:

18.1.1. Fornecedores Alternativos

18.1.1.1. Identificar e manter contato com fornecedores que possam assumir os serviços em caso de emergência.

18.1.1.2. Manter uma lista atualizada de fornecedores com capacidade de resposta rápida.

18.1.1.3. Desenvolver um plano claro para migrar para outro fornecedor em caso de falha da CONTRATADA.

18.1.2. Monitoramento Contínuo

18.1.2.1. Acompanhar o desempenho da CONTRATADA para identificar sinais de falha ou degradação dos serviços.

18.1.2.2. Estabelecer métricas de qualidade e alertas para indicadores críticos.

18.1.3. Comunicação Eficiente

18.1.3.1. Manter canais de comunicação claros entre o TRIBUNAL, a CONTRATADA e fornecedores alternativos.

18.1.3.2. Designar responsáveis pela coordenação em caso de ativação do plano de contingência.

18.1.4. Subscrições

18.1.4.1. Exigir que as subscrições do software antivírus tenham uma vigência mínima de 12 meses e estejam no nome do TRIBUNAL, de forma a ser possível utilizar as licenças ativadas até o final de sua vigência.

19. ESTRATÉGIA DE TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

19.1. **Atividades de Transição:** A transição para a nova solução deve ser feita de forma organizada, com foco na segurança e minimização de impactos. As principais etapas são:

19.1.1. Inventário de *Endpoint*s

19.1.1.1. Levantar todos os dispositivos protegidos (desktops, notebooks, servidores e dispositivos móveis) e os que deveriam estar, mas não estão protegidos pela solução.

19.1.1.2. Identificar as configurações e políticas de segurança atuais.

19.1.2. Migração de Configurações

19.1.2.1. Transferir as configurações e políticas da solução atual para a nova solução.

19.1.2.2. Garantir que todas as regras e exceções sejam aplicadas corretamente na nova plataforma.

19.1.3. Remoção Gradual da Solução Anterior (se aplicável)

19.1.3.1. Caso a nova solução seja diferente, remover a solução anterior de forma gradual, alinhada à implantação da nova solução.

19.1.3.2. Desinstalar a solução antiga apenas nos dispositivos onde a nova solução já estiver funcionando.

19.1.3.3. Verificar se não há resíduos da solução anterior que possam afetar o ambiente.

19.1.4. Documentação dos Processos

19.1.4.1. Documentar todas as configurações, políticas e procedimentos da solução atual e da nova solução.

19.1.4.2. Criar um manual de operações para a nova solução, incluindo monitoramento e resposta a incidentes.

19.2. **Atividades de Encerramento:** O encerramento do contrato deve garantir que a solução anterior seja removida com segurança (se aplicável) e que o ambiente permaneça protegido. As principais atividades são:

19.2.1. Remoção Gradual da Solução Anterior (se aplicável)

19.2.1.1. Remover a solução anterior apenas se a nova contratação for de uma solução diferente.

19.2.1.2. Fazer a remoção em etapas, acompanhando a implantação da nova solução.

19.2.1.3. Verificar se a desinstalação foi completa e sem resíduos.

19.2.2. Encerramento de Contas e Acessos

19.2.2.1. Revogar todos os acessos e credenciais da CONTRATADA ao ambiente do TRIBUNAL.

19.2.2.2. Encerrar contas de usuário e licenças associadas à solução anterior.

19.2.3. Verificação Técnica Pós-Encerramento

19.2.3.1. Realizar uma verificação técnica para garantir que a remoção da solução anterior (se aplicável) não deixou vulnerabilidades.

19.2.3.2. Documentar os resultados e entregar um relatório final ao TRIBUNAL.

20. ESTRATÉGIA DE INDEPENDÊNCIA

20.1. A contratação de um serviço gerenciado de segurança de *endpoint* envolve o pagamento recorrente para acesso ao software de segurança, suporte técnico, manutenção, atualizações, monitoramento proativo e resposta a incidentes. A CONTRATADA assume a gestão diária da solução, incluindo configuração, manutenção e proteção dos *endpoints*, enquanto o TRIBUNAL recebe relatórios regulares sobre o status da segurança. Esse modelo elimina a necessidade de

licenças perpétuas e permite que o TRIBUNAL tenha uma solução atualizada e gerenciada por especialistas, sem a complexidade e custos de se operar internamente.

20.2. Para garantir a independência do TRIBUNAL em relação à contratada, é essencial estabelecer cláusulas contratuais robustas, como a necessidade de as subscrições da solução terem uma vigência mínima de 12 meses e estarem em nome do TRIBUNAL.

20.3. Por fim, caso seja viável, a contratação deve incluir um plano de contingência para migração para outra solução em caso de falha da contratada, garantindo a continuidade das operações.

21.APROVAÇÃO E ASSINATURA

Integrante Técnico	**Integrante Demandante**
Paulo César da Silva CESEC	Márcio H. C. d'Ávila CESEC
Gestor Técnico	**Gestor Demandante**
Márcio H. C. d'Ávila CESEC	Alessandra da Silva Campos DIRTEC
O CECOR realizou a análise de conformidade do documento de acordo com Resolução nº 468/2022 do Conselho Nacional de Justiça.	
Guilherme da Silva Lourenço CECOR	Mateus Cançado Assis CECOR

Autoridade Máxima da Área de TIC (ou Autoridade Superior, se aplicável)
Alessandra da Silva Campos DIRTEC