TERMO DE REFERÊNCIA Nº 24471601 / 2025 - TJMG/SUP-ADM/DIRTEC/CESEC

1. ÁREA DEMANDANTE

Diretoria de Tecnologia da Informação e Comunicação - DIRTEC

2. OBJETO

Contratação de serviços gerenciados de segurança de *endpoint*, de natureza continuada, incluindo o fornecimento de solução de proteção, implantação, sustentação e serviços técnicos especializados.

3. FUNDAMENTO

A Importância da Segurança de *Endpoints* no TRIBUNAL

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

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.

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 a 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.

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.

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.

Contexto e Necessidade de Atualização

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:

1. A solução atualmente em uso não abrange servidores Linux, que fazem parte da infraestrutura central do TRIBUNAL.

2. A solução atualmente em uso não abrange dispositivos móveis do TRIBUNAL, tais como *tablets*.

3. Integração limitada com a plataforma de monitoramento de segurança cibernética atualmente utilizada pelo TRIBUNAL: A solução atualmente em uso não permite uma integração plena 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. Falta de serviços gerenciados, sustentação e suporte técnico: 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.

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

Situação Contratual da Solução Atualmente em Uso

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

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.

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

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.

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

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

4. ALINHAMENTO ESTRATÉGICO

A contratação da solução de TIC objeto deste Estudo Técnico Preliminar CONSTA NO PLANO ANUAL DE CONTRATAÇÕES da DIRTEC e está em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2025/2026) do TRIBUNAL, identificada no portfólio de ações através da ação estruturante de TIC (PDTIC) 10 - "Aquisição de Solução - Proteção Endpoint".

5. QUANTITATIVOS E PREÇOS MÁXIMOS

Item	Descrição do item	Código CATMAS	Quant.	Métrica	Preço Unitário Máximo	Preço Total Máximo
1	Serviço gerenciado de segurança de *endpoint* de natureza continuada, estimados para até 43.500 dispositivos em 36 meses	000112402	1.566.000	Dispositivos Mês	R$ 11,46	R$ 17.946.360,00
2	Serviço de implantação da solução	000112852	1	Unidade	R$ 92.169,00	R$ 92.169,00
3	Serviço técnico especializado de customização e apoio na solução, sob demanda, de natureza continuada, de até 600 horas por ano	000145645	1.800	Hora técnica	R$ 483,03	R$ 869.454,00

6. CARACTERÍSTICAS MÍNIMAS DO OBJETO

6.1 Características Mínimas do Objeto: Conforme ANEXO II.

6.2 Da Equipe Técnica: Conforme ANEXO III.

7. PRAZOS, LOCAL E CONDIÇÕES DE ENTREGA

O quadro a seguir apresenta os prazos máximos a partir da assinatura do contrato que poderão ser prorrogados a critério do TRIBUNAL e em comum acordo entre TRIBUNAL e CONTRATADA.

ETAPA	Evento	Prazo	Corrido/Útil	LOCAL
ETAPA 1 PREPARAÇÃO	1. Assinatura do contrato	D (marco)	-	SEI
	2. Início da execução contratual	D + 1	Dia útil	-
	3. Reunião de iniciação (*kick-off*) do: - contrato entre CONTRATADA e TRIBUNAL, juntamente com a indicação do respectivo preposto; - projeto de implantação da solução, juntamente com a indicação do respectivo gerente do projeto;	D + 5	Dia útil	Reunião presencial
	4. Preencher o Formulário de Análise de Perfil dos Contratados (referente ao Programa de Integridade do TRIBUNAL) [1]	D+30	Dia Corrido	-
ETAPA 2 IMPLANTAÇÃO	**Serviço de implantação da solução**			
	1. Disponibilização de infraestrutura básica da solução	D + 10 = P (marco)	Dia útil	
	2. Instalação dos agentes da solução em piloto nos *endpoints* do TRIBUNAL	P + 3	Meses	
	3. Documentação da solução e *workshop*	P + 4	Meses	
	4. Instalação dos agentes da solução em escala nos *endpoints* do TRIBUNAL	P + 6	Meses	
	5. Instalação dos agentes da solução nos *endpoints* residuais do TRIBUNAL	P + 9	Meses	
	Serviço de sustentação da solução			
	1. Início dos serviços de sustentação presencial no TRIBUNAL	P	-	DIRTEC em BH
	2. Início dos serviços de sustentação remoto	P	-	Remoto
	Serviço de customização da solução			

ETAPA 3 OPERAÇÃO CONTINUADA				
	3. TRIBUNAL emite uma ordem de serviço	O (marco)	-	
	4. CONTRATADA analisa a demanda e apresenta a proposta, com prazo/cronograma de execução e quantidade de horas técnicas necessárias	O + 3	Dias úteis	Remoto
	5. TRIBUNAL aprova ou rejeita a proposta da CONTRATADA	O + 6 = I (marco)	Dias úteis	
	6. Início da execução da ordem de serviço	I + 5	Dias úteis	
	7. CONTRATADA conclui a execução da ordem de serviço	Conforme cronograma	-	
	8. Recebimento provisório da entrega pelo TRIBUNAL	-	-	
	9. Recebimento definitivo da entrega pelo TRIBUNAL	5	Dias úteis	
	10. Reprovação da entrega pelo TRIBUNAL e solicitação de revisões, adequações ou correções	5	Dias úteis	
	11. CONTRATADA realiza ajustes solicitados	Ajustes pequenos: 5 Médios: 10 Grandes: 20	Dias úteis	

8. GARANTIA E/OU SUPORTE TÉCNICO

Conforme ANEXO II - Características Mínimas do Objeto.

9. NÍVEIS MÍNIMOS DE SERVIÇO - NMS

Conforme ANEXO IV - NMS.

10. FORMA DE EXECUÇÃO DOS SERVIÇOS

10.1. Início da prestação

10.1.1. A CONTRATADA deverá fazer uma reunião presencial para iniciação (*kick-off*) do contrato com o objetivo de alinhamento das expectativas contratuais e que deverá contemplar no mínimo:

10.1.1.1. Entrega do termo de sigilo e confidencialidade assinado, conforme modelo em ANEXO V - (Modelo) TERMO DE SIGILO - CONTRATADA;

10.1.1.2. Apresentação do preposto, informando endereço, telefone e e-mail;

10.1.1.3. Alinhamento dos procedimentos para cadastro do preposto como usuário externo do sistema SEI do TRIBUNAL para o recebimento de notificações e comunicações a respeito da execução do contrato;

10.1.1.4. Entrega da documentação exigida para a equipe que executará o serviço de sustentação presencial;

10.1.1.5. Questões relacionadas às ferramentas a serem utilizadas na abertura e acompanhamento dos serviços, padrões tecnológicos, modelos de artefatos necessários para a execução do contrato;

10.1.1.6. Alinhamento com o TRIBUNAL dos pontos de controle e acompanhamento da gestão do contrato, definindo periodicidade de entrega de informações gerenciais e de reuniões de acompanhamento;

10.1.1.7. Outros esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.

10.1.2. Para o início dos serviços de implantação da solução, a CONTRATADA deverá entregar o Plano de implantação, que deverá ser aprovado pelo TRIBUNAL.

10.1.3. A implantação deverá ser feita presencialmente pela equipe de implantação, específica para esta fase do projeto, com apoio das equipes de sustentação remota e presencial.

10.1.4. As subscrições da solução serão fornecidas e ativadas pela CONTRATADA conforme cronograma de instalação do agente da solução nos *endpoints*, ou seja, não terá um fornecimento único de todas as subscrições necessárias.

10.1.5. A instalação dos agentes nos *endpoints* ocorrerá de forma gradativa, conforme cronograma aprovado entre CONTRATADA e TRIBUNAL.

10.1.6. O serviço de customização será demandado através de ordens de serviço, conforme prazos estipulados no item Prazos, Local e Condições de entrega.

10.2 Indicadores

10.2.1. Os dados e as informações exibidas pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time).

10.2.3. Todos os indicadores exibidos pelo portal devem possuir a funcionalidade de detalhamento (drill down);

10.2.4. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo os níveis mínimos de serviços definido no presente termo de referência;

10.2.5. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos;

10.2.6. A qualquer tempo a CONTRATANTE poderá solicitar os dados brutos coletados das soluções informatizadas que compõem o objeto contratado.

11. REGRAS DE MEDIÇÃO E RECEBIMENTO DO OBJETO

11.1 O recebimento provisório é o recebimento das entregas dos serviços pelo TRIBUNAL para posterior análise e conferência se elas atendem às exigências do edital e seus anexos. Neste momento, o TRIBUNAL emite o termo de recebimento provisório.

11.2. O recebimento definitivo é dado pelo TRIBUNAL após verificar que as entregas estão em conformidade com as exigências do edital e seus anexos. Neste momento, o TRIBUNAL emite o termo de recebimento definitivo.

11.3 **Serviço gerenciado de proteção de *endpoint***

11.3.1. Deverão ser entregues, pela CONTRATADA, até o 5º (quinto) dia útil do mês subsequente à execução do serviço, os relatórios listados abaixo, sendo emitido neste momento pelo TRIBUNAL o termo de recebimento provisório:

11.3.1.1. Relatório de *endpoints* do TRIBUNAL com subscrição ativa da solução, conforme descrito no item "Fornecimento de uma solução de proteção de *endpoint*" do ANEXO II;

11.3.1.2. Relatório consolidado dos serviços remotos e presenciais de sustentação, conforme descrito no ANEXO II;

11.3.1.3. Relatório de NMS alcançados, conforme descritos no item 9 do TR.

11.4. **Serviço de implantação da solução**

11.4.1. O termo de recebimento provisório será emitido pelo TRIBUNAL após a conclusão das seguintes atividades:

11.4.1.1. Disponibilização de infraestrutura básica da solução, conforme descrito no ANEXO II.

11.4.1.2. Instalação dos agentes da solução em projeto piloto nos *endpoints* do TRIBUNAL e fornecimento da documentação da solução, juntamente com a realização do workshop, conforme descrito no ANEXOII;

11.4.1.3. Instalação dos agentes da solução em escala nos *endpoints* do TRIBUNAL, conforme descrito no ANEXO II.

11.5. **Serviço técnico especializado de customização e apoio na solução**

11.5.1. O termo de recebimento provisório será emitido pelo TRIBUNAL após a conclusão da Ordem de Serviço.

11.6. Após o recebimento provisório das entregas acima, o TRIBUNAL avaliará se elas atendem às especificações do edital e seus anexos, e em caso positivo, será emitido o termo de recebimento definitivo. Caso contrário, o TRIBUNAL emitirá termo de recusa, constando os ajustes ou correções a serem efetuados nas entregas.

11.7. O TRIBUNAL reserva-se o direito de solicitar quaisquer informações complementares necessárias para a avaliação das entregas efetuadas pela CONTRATADA e só emitirá o termo de recebimento definitivo quando todas as informações estiverem entregues, corretas e completas.

11.8. O faturamento de uma entrega só poderá ocorrer após a emissão do respectivo termo de recebimento definitivo dela.

12. FORMA DE PAGAMENTO E REAJUSTE

12.1. Serviço gerenciado de segurança de *endpoint*

12.1.1. O pagamento será feito mensalmente, no mês subsequente ao da prestação dos serviços, após a emissão, pelo TRIBUNAL, do termo de recebimento definitivo do serviço.

12.1.2. O pagamento do serviço gerenciado de segurança de *endpoint* inclui as subscrições em uso (ativas) pelo TRIBUNAL e os serviços de sustentação.

12.1.3 O pagamento será relativo à quantidade de subscrições ativas, ou seja, a quantidade de agentes instalados e ativos da solução nos *endpoints* do TRIBUNAL.

12.1.3.1. A CONTRATADA deve emitir um relatório com o quantitativo e seu respectivo detalhamento, de forma a possibilitar o cálculo do montante a pagar a partir do valor unitário da subscrição ativa e a quantidade de subscrições ativas no TRIBUNAL.

12.1.3.2. Para fins de comprovação, o relatório emitido deverá listar todos os *endpoints* com subscrição ativa, apresentando o nome, IP interno e outros dados que possibilitem a identificação do *endpoint* protegido.

12.1.4. Caso um *endpoint* deixe de requerer uma subscrição de proteção, esta poderá ser prontamente inativada, deixando com isso de ser contabilizada para o pagamento.

12.2. **Serviço de implantação da solução**

12.2.1. O pagamento será dividido em quatro parcelas e será realizado após a conclusão das atividades descritas abaixo e emissão, pelo TRIBUNAL, dos respectivos termos de recebimento definitivo.

12.2.2.

Atividade	**Percentual do valor total do serviço**
Disponibilização de infraestrutura básica da solução	20%
Instalação dos agentes da solução em piloto nos *endpoints* do TRIBUNAL	30%
Instalação dos agentes da solução em escala nos *endpoints* do TRIBUNAL	30%
Instalação dos agentes da solução nos *endpoints* residuais do TRIBUNAL	20%

12.3. **Serviço de customização da solução**

12.3.1. Os pagamentos serão realizados em parcela única, após a conclusão de cada ordem de serviço e emissão pelo Tribunal, do termo de recebimento definitivo.

12.3.2. O não atendimento às metas estabelecidas implicará em descontos (glosas) no pagamento, conforme definido no item 9 - Níveis Mínimos de Serviço.

12.4. Do Reajuste

12.4.1. Conforme disposições definidas na minuta do contrato.

13. OBRIGAÇÕES DA CONTRATADA

Conforme padrão do TRIBUNAL.

14. OBRIGAÇÕES DO TJMG

Conforme padrão do TRIBUNAL.

15. CONSÓRCIO OU SUBCONTRATAÇÃO

Não serão permitidos consórcio nem subcontratação.

16. GARANTIA CONTRATUAL

A CONTRATADA deverá ofertar garantia de 5% (cinco por cento) do valor anual do contrato.

17. VISITA TÉCNICA OU VISTORIA

Não há necessidade de visita técnica.

18. VIGÊNCIA DO CONTRATO

O prazo de vigência do contrato será de 36 (trinta e seis) meses, a contar da data da sua assinatura, prorrogável até o limite legal.

19. GESTÃO E FISCALIZAÇÃO DOS SERVIÇOS

19.1. O acompanhamento e fiscalização dos serviços objeto deste Contrato serão geridos pela Diretoria de Tecnologia da Informação de Comunicação – DIRTEC, atuando respectivamente como:

19.2. Gestores do contrato através do:

19.2.1. Assessor do Centro de Segurança Cibernética - CESEC;

19.2.2. Gerente da Gerência de Operações e Ativos de Tecnologia da Informação e Comunicação – GEOPE;

19.2.3. Gerente da Gerência de Operações e Ativos de Tecnologia da Informação e Comunicação - GETEC.

19.3. Cada um dos gestores do contrato nomeará formalmente um ou mais servidores para atuar como fiscal do contrato.

19.4. O acompanhamento e fiscalização deste Contrato pelo TRIBUNAL não excluem nem reduzem a responsabilidade da CONTRATADA pelo cumprimento das obrigações decorrentes deste instrumento.

19.5. Para tanto, o TRIBUNAL registrará as deficiências porventura existentes na execução dos serviços e/ou inobservância dos aspectos de segurança envolvidos, comunicando-as à CONTRATADA para a imediata correção, sem prejuízo da aplicação das penalidades cabíveis.

19.6. O TRIBUNAL, através do(s) Gestor(es) do Contrato, se reserva o direito de efetuar em qualquer tempo, nos serviços realizados pela CONTRATADA, auditoria e inspeção de qualidade.

19.7. A formalização da comunicação entre os gestores e/ou fiscais do TRIBUNAL e o preposto da CONTRATADA deverá ser realizada, preferencialmente, pelo Sistema Eletrônico de Informação – SEI do TRIBUNAL.

20. ANTICORRUPÇÃO

Conforme padrão do TRIBUNAL.

21. PROTEÇÃO DE DADOS PESSOAIS

Conforme padrão do TRIBUNAL.

22. SEGURANÇA DA INFORMAÇÃO

22.1. A CONTRATADA, seus empregados e consultores deverão manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto e informação de que tomar conhecimento em razão da execução do objeto do Contrato.

22.2. A CONTRATADA deverá providenciar a assinatura do Termo de Sigilo e Confidencialidade, conforme ANEXO V, pelo representante legal da empresa.

22.3. A CONTRATADA deverá assegurar que sejam firmados acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao contrato, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do Termo de Sigilo e Confidencialidade.

23. TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

23.1. A CONTRATADA deverá fazer transição final do contrato objetivando encerramento gradual dele, incluindo o repasse de conhecimento para a equipe técnica do TRIBUNAL, entrega de versões finais dos produtos, revogações de acesso e a diminuição gradual dos serviços que poderão ser executados por outra empresa Contratada ou pelo próprio TRIBUNAL no período de transição final.

23.1.1. O prazo da transição final será de no mínimo 3 (três) meses e no máximo 6 (seis) meses antes do encerramento da vigência do contrato.

23.1.2. O repasse do conhecimento será feito através do serviço técnico especializado de customização e apoio na solução. Durante o período de transição, a solução da CONTRATADA será desinstalada dos *endpoints*, à medida que a nova solução a ser contratada for sendo instalada nos mesmos.

23.1.3. O pagamento dos serviços será proporcional à quantidade de subscrições ativas nos *endpoints*.

23.1.4. Em até 1 (um) mês antes do início da transição final, o TRIBUNAL entregará à Contratada o Plano de Transição Final que conterá:

23.1.4.1. Escala gradativa de serviços que serão interrompidos até o encerramento contratual e correspondente cronograma de remuneração proporcional da Contratada.

23.1.4.2. Encerramento das licenças associadas à solução vigente.

23.1.4.3. Os produtos finais a serem entregues em suas últimas versões, tais como código fonte, executável, documentação, manuais, bem como todas as políticas, estratégias, planos, processos, procedimentos, configurações, regras, customizações, métricas, indicadores e painéis produzidos durante a vigência do contrato.

23.1.4.4. Quantidade de técnicos do TRIBUNAL para os quais será feito o repasse de conhecimento e quantidade de horas totais a serem utilizadas do banco de horas para esse objetivo.

23.1.4.5. Conteúdo programático do repasse de conhecimento.

23.1.5. Durante a transição final, os níveis mínimos de serviços continuarão a ser contabilizados para fins de deduções e para as sanções administrativas aplicáveis.

23.1.6. A Contratada deverá devolver todos os recursos materiais que foram disponibilizados pelo TRIBUNAL para a execução de suas atividades.

23.1.7. Todos os acessos, credenciais e caixas postais dos profissionais da CONTRATADA serão revogados imediatamente ao término da vigência do Contrato.

24. HABILITAÇÃO

24.1. **Qualificação Técnica**

24.1.1. Atestado(s) de capacidade técnico-operacional emitido(s) por pessoa jurídica de direito público ou privado em nome da LICITANTE, que comprove(m) experiência na prestação, de forma satisfatória, de Serviços Gerenciados de Cibersegurança e/ou Segurança da Informação similares aos especificados no Termo de Referência e seus anexos.

24.1.1.1. Serão considerados compatíveis os atestados que comprovem a prestação de Serviços Gerenciados de Cibersegurança e/ou Segurança da Informação, por pelo menos 12 (doze) meses, das seguintes parcelas de maior relevância:

24.1.1.1.1. Serviços gerenciados de proteção de *endpoints*, em ambiente com no mínimo 5.000 (cinco mil) ativos de tecnologia e contemplando no mínimo o fornecimento e sustentação de solução tecnológica especializada para proteção de *endpoints*;

24.1.1.1.2. Serviços gerenciados de segurança cibernética e/ou da informação, provendo estrutura dedicada e equipes de profissionais especializados, operando em regime contínuo e ininterrupto 24×7, prestados para ambiente com no mínimo 5.000 (cinco mil) ativos de tecnologia.

24.1.1.2. Será admitido o somatório de atestados em cada um dos itens acima para obtenção dos quantitativos exigidos, desde que pelo menos 01 (um) dos atestados contemple pelo menos 50% (cinquenta por cento) do total dos quantitativos.

24.1.1.3. Nos atestados deverão estar expressos, no mínimo, as seguintes informações:

24.1.1.3.1. Dados da empresa licitante: nome e CNPJ;

24.1.1.3.2. Dados da empresa cliente: nome e CNPJ;

24.1.1.3.3. Descrição dos serviços/fornecimento com dados que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;

24.1.1.3.4. Dados do emissor do atestado: nome e contato;

24.1.1.3.5. Data de emissão e assinatura do emissor.

24.1.1.4. O TRIBUNAL poderá promover diligências para dirimir quaisquer dúvidas, esclarecer ou complementar informações prestadas e aferir a veracidade das informações constantes nos atestados e documentos apresentados.

24.2. **Qualificação econômico-financeira**

24.2.1. Comprovação de patrimônio líquido no valor mínimo de 10% (dez por cento) do valor estimado para a contratação.

25. ACEITABILIDADE DA PROPOSTA

25.1. Além da documentação de Habilitação, como condição de aceitabilidade da proposta, na etapa de julgamento das propostas para a classificada em primeiro lugar, a LICITANTE deverá apresentar também:

25.1.1. Detalhamento das soluções informatizadas, por planilha “ponto a ponto” de comprovação do atendimento a cada item da especificação das soluções informatizadas, indicando a documentação técnica (manual técnico, catálogo técnico, datasheet, folha de dados ou folha de especificações, artigo de conhecimento de suporte técnico e similares do fabricante, divulgados de forma ampla e oficial ao mercado), a página e/ ou tópico onde se encontra cada informação, ou, alternativamente, imagens das interfaces gráficas das soluções que comprovem o atendimento do requisito:

25.1.1.1. Anexo II, 2.1.4 “Gestão centralizada” e seus subitens;

25.1.1.2. Anexo II, 2.1.5 “Alertas e relatórios” e seus subitens;

25.1.1.3. Anexo II, 2.1.6 “Critérios gerais para proteção de *endpoints*” e seus subitens;

25.1.1.4. Anexo II, 2.1.7 “Redução da superfície de ataque” e seus subitens;

25.1.1.5. Anexo II, 2.1.8 “Técnicas de proteção de *endpoint* em pré-execução” e seus subitens;

25.1.1.6. Anexo II, 2.1.9 “Técnicas de proteção de *endpoint* em execução (peri-execução)” e seus subitens;

25.1.1.7. Anexo II, 2.1.10 “Técnicas de detecção e resposta em pós-execução (*Endpoint Detection and Response* - EDR)” e seus subitens;

25.1.1.8. Anexo II, 2.1.11 “Proteção de rede” e seus subitens.

25.2. O pregoeiro poderá, subsidiado pelo apoio técnico e como condição de aceitação da proposta, solicitar à LICITANTE classificada em primeiro lugar que se submeta à realização de uma Prova de Conceito - POC para comprovar o pleno atendimento de requisitos para os quais restem eventuais dúvidas, a serem enumerados pelo TRIBUNAL.

25.2.1. O pregoeiro irá agendar data e horário, com antecedência de até 10 (dez) dias úteis, para que a LICITANTE apresente a prova de conceito.

25.2.2. Qualquer alteração de data e horário será devidamente informada no chat, podendo ocorrer postagens diárias.

25.2.3. A POC será realizada em ambiente preparado pela licitante e apresentada de forma on-line, para que a LICITANTE demonstre a comprovação do atendimento dos requisitos enumerados, conforme as especificações exigidas no edital e seus anexos;

25.2.4. Serão de inteira responsabilidade da LICITANTE todas as despesas para a preparação e apresentação da POC;

25.2.5. A LICITANTE que não apresentar a POC na data estabelecida, ou que apresentar POC que não atenda às exigências do edital, terá sua proposta desclassificada.

26. MODELO DE PROPOSTA COMERCIAL

26.1. O LICITANTE deverá apresentar proposta comercial conforme modelos constantes do ANEXO VI deste edital.

26.2. O LICITANTE deverá informar na proposta comercial, o fabricante dos produtos ofertados, marca, modelo, part number, descrição técnica.

27. SANÇÕES

27.1. Conforme padrão do TRIBUNAL.

27.2. **Das multas moratórias**

27.2.1. **Moratória** de até 0,3% (três décimos por cento) sobre o valor da parcela inadimplida, por dia de atraso, até o trigésimo dia de atraso.

27.2.2. **Moratória** de até 20% (vinte por cento) sobre o valor da parcela inadimplida em caso de atrasos injustificados superiores a 30 (trinta) dias ou fornecimento com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminuam-lhe o valor ou, ainda, fora das especificações contratadas.

27.2.3. **Moratória** de até 2% (dois por cento) sobre o valor total do contrato, em caso de descumprimento das demais obrigações contratuais ou normas da legislação pertinente.

27.2.4. **Moratória** de 0,1% (um décimo por cento) por dia de atraso injustificado, sobre o valor do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação suplementação ou reposição da garantia.

28. ASSINATURAS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Técnico	Integrante Demandante
Paulo César da Silva CESEC	Márcio H. C. d'Ávila CESEC

29. APROVAÇÃO DA AUTORIDADE MÁXIMA DA DIRTEC

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

---

[1] Programa de Integridade do TRIBUNAL, https://www.tjmg.jus.br/portal-tjmg/acoes-e-programas/programa-de-integridade.htm

Documento assinado eletronicamente por **Márcio Henrique Camargos D''Ávila**, **Assessor(a) Técnico(a)**, em 28/10/2025, às 17:14, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.