



## TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

### SG-STI-CIN-DSUST - DIVISÃO DE SUSTENTAÇÃO DA COORDENADORIA DE INFRAESTRUTURA E OPERAÇÕES DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Nº SEI/TJPR 0092647-64.2025.8.16.6000  
Nº SEI-DOC 13070564

## TERMO DE REFERÊNCIA

### 1. OBJETO

1.1. Solução de TIC para proteção de dados composta por subscrição de licenciamento de software, servidores, serviços de instalação, configuração, capacitação, sustentação e suporte técnico especializado e garantia por um período de 60 (sessenta) meses.

#### 1.1.1. ESPECIFICAÇÃO DETALHADA DO OBJETO

Item	Serviço	CATMAT/ CATSER	Descrição	Unidade	Quant.	Volumetria Unitária	Volumetria Total
1	27502	CATSER	Software de Proteção de Dados	Software de Proteção de Dados	1	-	-
2	485937	CATMAT	Servidor de Armazenamento de alta performance	Servidores	4	100 TB	400 TB
3	618356	CATMAT	Appliances de Armazenamento de alta densidade	Terabytes	2	500 TB	1.000 TB
4	26972	CATSER	Serviço - Instalação, Configuração e Migração dos Jobs	Serviço	1		
5	03840	CATSER	Serviço – Capacitação no Software de Proteção de Dados para 12 pessoas	Serviço	1	-	-
6	16837	CATSER	Serviço – Capacitação no Appliances de Armazenamento de alta densidade para 12 pessoas	Serviço	1		
7	27022	CATSER	Serviço de Gerenciamento Técnico e Sustentação da Solução de Proteção de Dados *	Meses	Até 60	-	-
8	27022	CATSER	Serviço - Horas Técnicas Especializadas sob demanda	Horas	1.000	-	-

\* O início da prestação do serviço ocorrerá mediante solicitação e a partir da entrega dos itens 1,2 e 3, conforme DINÂMICA DE EXECUÇÃO.

## **1.2. NATUREZA DO OBJETO**

1.2.1. O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

1.2.2. Por se tratar de bens usuais no mercado, oferecido por alguns fabricantes no mercado e passíveis de serem definidos de forma objetiva, o objeto em questão se enquadra na definição de bens e serviços comuns, conforme a Decreto Estadual nº 10.086/2022.

1.2.3. Toda a solução contará com garantia, suporte e subscrição por 60 (sessenta) meses, com exceção do serviço de horas técnicas especializadas que será de 120 (cento e vinte) dias.

## **1.3. DESCRIÇÃO DA SOLUÇÃO**

1.3.1. A solução proposta para o Tribunal de Justiça do Estado do Paraná (TJ/PR) consiste em um conjunto integrado de tecnologias e serviços que asseguram a proteção completa dos dados institucionais, garantindo alta disponibilidade, escalabilidade, segurança e conformidade com as normas legais e estratégicas vigentes.

### **1.3.2. Componentes Tecnológicos:**

- **Software de Proteção de Dados:** Plataforma avançada para gerenciamento de *backup* e restauração, com recursos de deduplicação, criptografia, proteção contra *ransomware* e integração com ambientes modernos (máquinas virtuais, Kubernetes, nuvem e soluções híbridas). Essa camada é responsável por orquestrar políticas de proteção, monitoramento e recuperação rápida, assegurando a continuidade dos serviços judiciais.
- **Servidor de Armazenamento de alta performance:** Infraestrutura otimizada para operações críticas de *backup* e restauração, garantindo velocidade e confiabilidade na execução dos processos. Ideal para dados de alta rotatividade e sistemas que exigem respostas imediatas.
- **Appliances de Armazenamento de alta densidade:** Equipamentos dedicados para armazenamento massivo, com alta capacidade e eficiência energética, destinados à retenção de longo prazo e à escalabilidade da solução. Essa camada complementa a estratégia de proteção 3-2-1-0, assegurando redundância e resiliência.

### **1.3.3. Serviços Associados:**

- **Instalação e Configuração:** Implementação completa da solução, incluindo integração com os ambientes existentes e validação funcional.
- **Capacitações e Transferência de Conhecimento:** Capacitação da equipe técnica do TJ/PR para operação, manutenção e evolução da solução.
- **Migração dos Jobs:** Transferência segura dos processos de backup atuais para a nova plataforma, com testes de restauração para garantir integridade.
- **Gerenciamento Técnico e Sustentação:** Monitoramento contínuo, suporte especializado 24x7 e aplicação de boas práticas de governança.
- **Horas Técnicas Especializadas sob Demanda:** Atendimento a necessidades específicas, como ajustes avançados, consultoria e otimizações.

### **1.3.4. Benefícios da Solução Integrada:**

- **Segurança e Conformidade:** Atende às exigências da Lei 14.133/2021, Resolução CNJ 468/2022 e Guia de Contratações de TI do CNJ.
- **Alta Disponibilidade e Resiliência:** Reduz riscos de indisponibilidade e perda de dados, garantindo continuidade operacional.
- **Escalabilidade e Sustentabilidade:** Preparada para crescimento futuro e alinhada às práticas ambientais.
- **Eficiência Operacional:** Integração completa entre software, hardware e serviços,

com suporte especializado e SLA rigoroso.

1.3.5. Essa arquitetura integrada assegura que o TJ/PR disponha de uma solução moderna, robusta e aderente às melhores práticas do setor público, garantindo proteção, governança e evolução tecnológica ao longo do ciclo contratual.

#### **1.4. PARCELAMENTO E ADJUDICAÇÃO DO OBJETO**

1.4.1. Os itens que compõem a solução proposta são interdependentes, e o seu parcelamento pode acarretar prejuízos tanto econômicos quanto operacionais. Por essa razão, recomenda-se que a contratação seja realizada em lote único, no qual uma única empresa será responsável pelo fornecimento de todos os softwares, hardwares e serviços previstos no objeto da licitação, conforme as seguintes justificativas:

1.4.2. Mercado: Verificou-se que existem empresas com capacidade para fornecer integralmente todos os serviços solicitados, demonstrando a viabilidade da contratação de um único fornecedor que atenda a todas as demandas.

1.4.3. Técnico: Os itens definidos para esta contratação apresentam forte inter-relação. A subdivisão dos serviços em múltiplos lotes exigiria alinhamento entre diferentes empresas vencedoras, aumentando a complexidade operacional, dificultando a responsabilização em caso de falhas e tornando a gestão de múltiplos fornecedores mais onerosa. Tal fragmentação comprometeria a eficiência da operação e da manutenção da solução como um todo, exigindo maior esforço de gestão.

1.4.4. Financeiro: A divisão dos itens em lotes não proporcionaria ganhos de economia de escala, pois os lotes poderiam ser ofertados por uma única empresa. Além disso, determinados lotes podem não ser atrativos sob o aspecto econômico-financeiro, reduzindo a competitividade e, consequentemente, elevando o custo global da prestação dos serviços.

1.4.5. Gestão: A contratação de várias empresas aumentaria os custos administrativos, especialmente nas atividades de análise, verificação e contestação de faturas. A gestão de um contrato único facilita o acompanhamento e o controle dos serviços contratados, garantindo maior eficiência.

1.4.6. Diante do exposto, considerando a forte interdependência entre os itens e a recomendação técnica de não parcelar esses componentes, sugere-se que a adjudicação seja realizada de forma integral, para um único fornecedor, assegurando eficiência técnica, financeira e gerencial.

1.4.7. Considerando que não se recomenda o parcelamento, a adjudicação do objeto da presente contratação deverá ocorrer em favor de um único fornecedor, garantindo melhor atendimento à demanda, bem como suporte e garantia adequados. Ademais, não se recomenda a reserva de cotas para Microempresas ou Empresas de Pequeno Porte (ME/EPP), pois tal medida poderia resultar na contratação de múltiplas empresas, dificultando a gestão e fiscalização contratual e ocasionando transtornos operacionais, especialmente relacionados aos procedimentos de garantia técnica, licenciamento e implantação da solução.

## **2. FUNDAMENTOS DA CONTRATAÇÃO**

### **2.1. REFERÊNCIA AOS ESTUDOS TÉCNICOS PRELIMINARES**

2.1.1. Este termo de referência foi elaborado considerando os Estudos Preliminares de STIC 13026686.

### **2.2. MOTIVAÇÃO**

2.2.1. Considerando as diretrizes estabelecidas no Planejamento Estratégico do Tribunal de Justiça do Paraná para o período de 2021-2026, ratificado pela Resolução N.º 300-OE de 09/08/2024, sob o qual destacamos o objetivo estratégico 12 "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados" que intenciona assegurar a infraestrutura adequada ao funcionamento do TJPR, para isso é imprescindível a realização de investimentos em Tecnologia da Informação e Comunicação (TIC) com o propósito de modernizar sua infraestrutura e atingir as metas estipuladas. Ademais, conforme estabelecido pela Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), é necessário aperfeiçoar a Segurança da Informação e a Gestão de Dados, bem como promover Serviços de Infraestrutura e Soluções Corporativas para suprir as demandas e assegurar o funcionamento adequado do TJPR, impulsionando a implantação e

o aprimoramento contínuo dos sistemas judiciais e fornecendo infraestrutura tecnológica apropriada às atividades judiciais e administrativas.

2.2.2. A utilização da Tecnologia da Informação como instrumento de otimização das atividades administrativas permite que os órgãos da Administração Pública elaborem medidas que tornem seus procedimentos cada vez mais ágeis, seguros, integrados, eficientes e, sobretudo, acessíveis a toda a população brasileira.

2.2.3. O aumento do volume de dados gerados e utilizados por aplicações, serviços de e-mail, bases de dados e servidores de arquivos recai sobre a utilização dos armazenamentos *on-premises* instalados no data center da instituição. A preservação desses dados deve ser realizada de forma segura e estar sempre disponível quando necessário.

2.2.4. Hoje, a solução de backup em uso é composta pela associação de três produtos: Software de *Backup/Restore*, Equipamento de *backup* em disco e Biblioteca de armazenamento em fitas, os quais são evidenciados na tabela a seguir:

Item	Tipo de Dispositivo	Quantidade	Contrato	Documento	SEI	Vencimento
1	Software de Backup	1	320/2018	3425079	0071352-49.2017.8.16.6000	10/03/2023
2	Backup em Disco (Quantum DX)	2	125/2017	2354775	0056252-54.2017.8.16.6000	14/07/2022
3	Backup em Disco (Dell Data Domain)	2	431/2019	4508917	0062631-74.2018.8.16.6000	13/12/2024
4	Biblioteca de armazenamento em fitas	2	433/2019	4509136	0062631-74.2018.8.16.6000	12/02/2025

Lista de produtos, serviços, contratos e vencimentos da solução de backup.

2.2.5. Os equipamentos atuais encontram-se em processo de renovação de suporte e garantia (SEI nº0029425-93.2023.8.16.6000); contudo, essa cobertura permanece restrita aos itens já protegidos.

2.2.6. Por padrão os ativos de TIC são adquiridos em pares, com a finalidade de alocá-los proporcionalmente em cada Datacenter, seguindo o conceito de alta disponibilidade.

2.2.7. No que concerne à área de armazenamento em uso, registra-se a utilização total de 500 TB entre todos os equipamentos de backup em discos. Embora existam em torno de 470 TB livres para armazenamento, é necessário considerar que estamos em um ecossistema de alta disponibilidade. Isso implica que, caso um ambiente esteja completamente inativo, o outro deverá ser capaz de sustentar toda a infraestrutura de TIC necessária para a continuidade dos serviços deste Tribunal de Justiça.

2.2.8. Por sua vez, em relação às fitas de backup adquiridas em conjunto com a biblioteca de armazenamento, não se pode quantificar o número de unidades em uso ou disponíveis, uma vez que é possível reutilizar as fitas após a expiração do conteúdo nelas armazenado. As unidades de gravação, bem como as fitas, estão na geração 7 lançada em 2015, denominada "LTO 7" (*Linear Tape-Open*), com capacidade máxima de gravação de 6 Tb.

2.2.9. Nos últimos anos, o Tribunal de Justiça do Paraná adotou a tecnologia de contêineres conhecida como *Kubernetes*, ou simplesmente K8S, como base para todos os sistemas, acompanhando uma tendência de mercado com o intuito de otimizar o uso da infraestrutura.

2.2.10. A solução de backup atual não suporta backups de K8S, uma vez que, no momento da contratação, essa tecnologia ainda não estava sendo considerada para utilização em ambientes de produção.

2.2.11. Outra funcionalidade que não é plenamente atendida pela solução de backup atual é a capacidade de realizar cópias de segurança de máquinas virtuais. Essa necessidade tornou-se evidente à medida que equipamentos legados foram migrados para máquinas virtuais, como ocorreu com os bancos de dados Caché e Sybase, que atualmente prestam serviço de consulta para os sistemas de Infância e Juventude, Juizado de Menores, Comissão Estadual Judiciária de Adoção, Consulta de Comarcas, Cartórios e Distritos, Controle de DNA, Controle de Testamento, Judwin e Recursos Humanos.

2.2.12. Acrescenta-se ainda que, a pandemia de Covid-19 exigiu um esforço significativo das organizações para disponibilizar suas aplicações 24/7/365 na internet, sendo a adoção de serviços em nuvem o meio mais ágil para tal finalidade. O Tribunal de Justiça, por exemplo, estabeleceu o uso do Microsoft Teams como ferramenta oficial para videoconferências e audiências, conforme os processos SEI nº 0083859-37.2020.8.16.6000, nº 0118143-71.2020.8.16.6000 e Despacho nº 5831110, divulgados no Ofício-Circular Nº 157/2020. Contudo, essa é apenas uma das funcionalidades do Teams. A referida aplicação interage diretamente com o Microsoft SharePoint (Sites e Arquivos) e o Microsoft Exchange (E-Mail), ambos em processo de migração para a nuvem ou já migrados. Nesse contexto, a própria Microsoft recomenda o backup das informações contidas nestes aplicativos, conforme pode ser verificado no [Service Availability](#), do qual segue excerto.

6. Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. **We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.**

2.2.13. No art.º 38 da resolução CNJ 370/2021 está prescrito que os órgãos devem elaborar e implementar práticas e processos voltados à segurança da informação e à proteção de dados. A partir desta determinação, esta área demandante consultou a Divisão de Gestão da Segurança da Informação sobre a possibilidade de considerar a solução de cópia de segurança (*backup/restore*) estratégica e portanto a manutenção de suporte, garantia e subscrição deste serviço (Cota SEI nº 10473765), o qual foi respondido na Cota SEI nº 10486322, de onde se extrai o texto a seguir:

1. As sugestões apresentadas são pertinentes para a contratação de solução de cópia de segurança, trazendo a definição de elementos importantes para garantia, suporte técnico especializado e subscrição, uma vez que esta solução apoia diretamente a Continuidade dos Serviços Essenciais de TIC do Tribunal.

2. Entendemos também que as sugestões são relevantes ao ponto de serem consideradas no prisma de um escopo maior, podendo ser incluída em normativas relacionadas a contratação de TIC e terceirizações, principalmente para soluções que apoiam os Serviços Essenciais de TIC do Tribunal.

3. Enquanto não há normativa oficial para este fim, recomenda-se que todas as Divisões da SETI que realizam processos de contratação avaliem, sempre que possível, à inclusão dos itens sugeridos na cota 10473765 em seus processos de contratação.

2.2.14. Tal recomendação foi ratificada pelo Secretário de Tecnologia da Informação - Em exercício na Manifestação 10518413.

2.2.15. Nesta seara, o Conselho Nacional de Justiça publicou a Resolução 396/2021, a qual "Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)". Essa resolução tem como objetivos o disposto no Artigo 6º:

I – tornar o Judiciário mais seguro e inclusivo no ambiente digital;

II – aumentar a resiliência às ameaças cibernéticas;

III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e

IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

2.2.16. Nos últimos anos, a utilização do conceito 3-2-1-0 para soluções de proteção de dados, tem se consolidado como uma forma eficaz para este tipo de serviço, especialmente no contexto de *backup* e restauração. Essa abordagem tornou-se amplamente reconhecida e recomendada. O princípio central da estratégia é simples: manter pelo menos **três** cópias dos seus dados, armazená-las em **dois** tipos diferentes de mídia, garantir que **uma** dessas cópias esteja localizada fora do local físico principal (*offsite*) e **zero** erros encontrados durante o teste de backup. Essa metodologia ajuda a mitigar riscos associados a falhas de hardware, erros humanos, ataques de *ransomware* e desastres naturais, proporcionando uma camada adicional de segurança e confiabilidade.

2.2.17. A primeira regra sugere ter três cópias dos dados: a cópia original e duas cópias de *backup*. Isso garante que, mesmo que uma cópia seja comprometida, outras duas estarão disponíveis para recuperação. Em segundo lugar, os dados devem ser armazenados em dois tipos diferentes de mídia, como discos rígidos internos e externos, fitas ou armazenamento em nuvem. Essa diversidade de mídia é importante para evitar a falha total de um único tipo de armazenamento. Finalmente, manter uma cópia dos dados fora do local principal (*offsite*) é crucial para proteger contra desastres que possam afetar a infraestrutura física local, como incêndios, enchentes ou roubo, por fim a ausência de erros em testes de recuperabilidade executados sobre os dados protegidos.

2.2.18. A estratégia 3-2-1-0 é amplamente aceita por especialistas em TI e segurança da informação como uma prática recomendada para garantir a resiliência dos dados. Adotar essa estratégia pode aumentar significativamente a probabilidade de recuperação de dados em caso de incidentes. Fabricantes como a [Coomvault](#), [IBM](#), [Veeam](#), e a [Veritas](#) e revistas especializadas [ComputerWeekly](#) e [TechTarget](#) oferecem informações detalhadas sobre a implementação e os benefícios dessa abordagem.

2.2.19. Portanto, a realização desse estudo permitirá ao Tribunal de Justiça do Paraná identificar e adotar as soluções mais adequadas, assegurando a continuidade dos serviços e a proteção das informações críticas, contribuindo assim para o bom funcionamento do sistema judiciário e a promoção da justiça, uma vez que uma solução de cópia de segurança representa a última linha de defesa em termos de segurança, e sua inexistência ou falha pode resultar na perda irreversível de informações.

2.2.20. A ampliação de uma solução de backup para uma solução de proteção de dados mais abrangente é essencial para garantir a continuidade do negócio em um cenário em que a segurança da informação se torna cada vez mais crítica. Enquanto o backup tradicional foca na recuperação de dados após um incidente, uma solução de proteção de dados inclui não só a recuperação, mas também a prevenção contra perda, corrupção e roubo de informações, além de garantir a conformidade regulatória, como exigido por leis como a LGPD e o GDPR. A implementação de medidas como criptografia, monitoramento contínuo e recuperação rápida em caso de ataque cibernético são fundamentais para proteger a integridade dos dados, minimizar o tempo de inatividade e, conseqüentemente, preservar a continuidade operacional.

2.2.21. Estudos mostram que empresas que sofrem perdas significativas de dados ou interrupções prolongadas enfrentam impactos financeiros severos e até o risco de falência. Assim, evoluir para uma solução robusta de proteção de dados não é apenas uma questão de segurança, mas uma estratégia de negócio para manter a resiliência frente a ameaças cibernéticas cada vez mais sofisticadas e garantir a continuidade das operações. Segundo o [Ponemon Institute](#) - renomado centro de pesquisa dedicado à privacidade, proteção de dados e segurança da informação - o custo médio de uma violação de dados pode atingir milhões de dólares, além de causar uma significativa degradação da reputação. Esse cenário ressalta a importância de adotar uma abordagem mais proativa e abrangente na proteção das informações.

2.2.22. Um ponto importante merecedor de destaque é que, atualmente, a equipe responsável pela solução de backup e restauração também é responsável pelos equipamentos de armazenamento. Essa prática não é recomendada pelo mercado, pois a organização corre risco ao designar a mesma equipe para armazenar as informações e gerenciar as cópias de segurança. Isso pode resultar em possíveis falhas nos processos de manipulação e gerenciamento dos equipamentos, além de comprometer a segregação de responsabilidades, fundamental para garantir a segurança dos dados. De tal sorte, que a partir da implantação desta solução a responsabilidade pela solução de proteção de dados recairá à Divisão de Sustentação, vinculada a Coordenação de Infraestrutura e Operações.

2.2.23. Nesta toada, ressalta-se que este Tribunal de Justiça não possui, na sua estrutura de [cargos/salários](#), um específico para Analista de Backup, profissional responsável por planejar, gerenciar e manter a infraestrutura de backup de uma organização. Entre suas principais atividades estão:

- Selecionar, implantar e manter hardwares e software
- Controlar o acesso aos recursos
- Planejar, criar, manter, executar, atualizar, testar e documentar as rotinas de backup

- Acompanhar o desempenho dos recursos técnicos
- Gerenciar a restauração dos dados
- Otimizar os recursos de armazenamento
- Identificar e resolver incidentes
- Planejar, criar, manter e executar as políticas de proteção de dados
- Elaborar relatórios gerenciais
- Elaborar documentações de evidências de backup, restauração e relacionado a saúde dos ativos da solução de proteção dados
- Planejar, desenhar, criar, manter, atualizar, executar, testar e documentar o processo de recuperação em casos de desastres.

2.2.24. Por fim, é importante destacar que, na tramitação do expediente nº 0107633-28.2022.8.16.6000, objetivou-se a aquisição de uma solução de proteção de dados, contemplando softwares, hardwares, serviços de operação e armazenamento em nuvem, organizada em três grupos:

- Grupo 1: Software e *appliances* de backup
- Grupo 2: Equipamento de armazenamento objeto
- Item 8: Serviço de armazenamento objeto em nuvem

2.2.25. Após a conclusão das etapas do processo licitatório no âmbito do TJPR, foi autorizado o Pregão Eletrônico nº 50/2025, agendado para 06/11/2025, às 13h30, conforme Edital assinado (SEI nº 12314532).

2.2.26. Esse pregão foi submetido à inspeção prévia do Tribunal de Contas do Estado do Paraná (TCE/PR), por meio da demanda Id 473, AF 3347 (2025), Despacho SEI nº 12350966. Em 05/11/2025, por volta das 18h, a Secretaria de Tecnologia da Informação tomou conhecimento do **Achado 1** (Anexo – SEI nº 12383175), cujo campo “Condição” apresentava a seguinte análise:

Da análise ao Edital da licitação em referência, constatou-se que os Itens 3 (“Serviço – Instalação, Configuração, Capacitação e Migração dos Jobs”) e 4 (“Serviço – Gerenciamento Técnico e Sustentação de Armazenamento e Backup”), apresentam valores totais de R\$ 102.179,20 e R\$ 775.104,00, respectivamente, correspondendo a montantes inferiores a 4% do valor global estimado da contratação (R\$ 2.126.096,06).

Nos termos do art. 67, § 4º, da Lei nº 14.133/2021, somente podem ser exigidos atestados de capacidade técnica para parcelas de maior relevância do objeto, definidas como aquelas cujo valor seja superior àquele percentual (4%).

**Assim, a exigência de atestado para esses itens configura desconformidade legal, por abranger parcelas que não se enquadram como de maior relevância, o que pode gerar restrição indevida à competitividade e violação ao princípio da legalidade.** (Grifo nosso)

2.2.27. Diante do achado, a equipe de planejamento deliberou pela revogação da exigência de atestado de capacidade técnica para os Itens 3 e 4 do Grupo 1 (Informação SEI nº 12384657). Todavia, em razão do exíguo prazo entre a comunicação do achado e o início do pregão, optou-se por incluir aviso na plataforma de compras governamentais.

2.2.28. Devido à alteração substancial (remoção da exigência de atestado de capacidade técnica) e à realização do pregão eletrônico 50/2025 em 06/11/2025, decidiu-se manter a aquisição do grupo 2 e item 8, e republicar o edital para o grupo 1. Para tanto, foi emitido o Parecer Jurídico SEI nº 12391842, elaborado pela Consultoria Jurídica do Gabinete do Secretário da Secretaria de Tecnologia da Informação.

## 2.3. OBJETIVOS e BENEFÍCIOS

2.3.1. Dar continuidade ao serviço de proteção de dados.

2.3.2. Ampliar o número de ativos de TIC cobertos pelo serviço de proteção de dados.

2.3.3. Alinhar-se às melhores práticas de mercado em serviços de proteção de dados.

2.3.4. Tornar o serviço de proteção de dados mais resiliente, seguindo o conceito de alta disponibilidade.

2.3.5. Melhorar a qualidade do serviço de proteção de dados oferecido aos responsáveis pela informação.

## 2.4. ALINHAMENTO ESTRATÉGICO

### 2.4.1. PEI - Planejamento Estratégico do Poder Judiciário (PEI 2021 – 2026)

2.4.1.1. A contratação objeto deste estudo visa atender aos seguintes Objetivos Estratégicos Institucionais, constantes no Plano Estratégico Institucional vigente:

02 – Fortalecimento da Relação Institucional do Judiciário com a Sociedade;

12 – Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

### 2.4.2. PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)

2.4.2.1. A contratação objeto deste estudo visa atender aos seguintes Objetivos Estratégicos, constantes no Plano Diretor de Tecnologia da Informação e Comunicação vigente:

OE.TIC-3: Modernizar e fortalecer a infraestrutura tecnológica para suporte e segurança das operações do Tribunal;

## 2.5. ANÁLISE DE MERCADO DE TIC

### 2.5.1. CONTRATAÇÕES SIMILARES

2.5.1.1. Encontram-se identificadas na tabela abaixo as contratações realizadas por outros órgãos ou entidades da Administração Pública, cuja necessidade ou problema se assemelham à necessidade objeto deste estudo, contudo ressalva-se que por tratar-se de solução apropriada as demandas do TJPR, não existe total similaridade:

Órgão	Contrato	Solução	Valor
TCE/RJ	Pregão nº 00018/2023 Termo de Homologação e Proposta Recompota (SEI doc. nº 12695402)	Área de armazenamento de alta densidade	R\$ 3.187.000,00
TJPR	Pregão Eletrônico nº 64/2023 Proposta Recompota (SEI doc. nº 9972353)	Horas Técnicas Especializadas sob demanda	R\$ 330,88
STJ	Contrato STJ N. 104/2025 (SEI doc. nº 12695443)	Fornecimento de solução de "appliances" de backup de longa retenção, em Disco.	R\$ 2.360.000,00
TJGO	Contrato Nº 58/2025 (SEI doc. nº 12695464)	Solução de cópia de segurança Veritas Netbackup, tendo como finalidade garantir o backup dos dados dos sistemas computacionais	R\$ 3.837.296,00
CJF	Contrato CJF nº 007/2024 (SEI doc. nº 12695487)	solução de backup de dados, contemplando a subscrição de licenciamento de software e o fornecimento de equipamento(s), serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia.	R\$ 8.943.700,00
Detran/RJ	Contrato Detran/RJ nº 492/2025 (SEI doc. nº 12695503)	Aquisição de solução de appliances de backup em cluster do fabricante Exagrid, com Garantia de manutenção do fabricante por 60 (sessenta) meses	R\$ 31.242.148,16

### 2.5.2. SOLUÇÕES DE SOFTWARE LIVRE OU PÚBLICO

2.5.2.1. Não foram localizadas soluções de Software Livre ou Público que se referem à necessidade deste estudo.

### 2.5.3. SOLUÇÕES DISPONÍVEIS NO MERCADO



2.5.3.1. Segundo o Ministério da Gestão e da Inovação em Serviços Públicos, uma solução de TIC consiste em um conjunto integrado de tecnologias, sistemas, softwares, hardwares e serviços que, combinados, atendem a necessidades específicas do negócio, otimizam processos, aprimoram a comunicação e a gestão da informação, visando aumentar a eficiência e a produtividade organizacional. Essa solução abrange desde a infraestrutura - como redes e servidores - até aplicações avançadas, incluindo Inteligência Artificial, Computação em Nuvem, segurança de dados e suporte ao usuário, tudo voltado para apoiar as operações e subsidiar a tomada de decisão. Assim, cada instituição pode desenvolver uma solução de proteção de dados adequada às suas necessidades, avaliando as tecnologias disponíveis no mercado e garantindo alinhamento ao seu orçamento. (<https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/orientacoes-e-apoio-especializado/conceito-de-solucao-de-tic>)

2.5.3.2. Considerando a realização do Pregão Eletrônico nº 50/2025, em 06/11/2025, no qual foram adquiridos o Grupo 2 – Solução de Armazenamento Objeto e o Item 8 – Serviço de Armazenamento em Nuvem, não foi realizada a avaliação dessas duas tecnologias.

Nesse contexto, passaremos a analisar os bens e/ou serviços que podem compor a solução a ser contratada, referindo-nos a cada um deles como "tecnologia".

2.5.3.3. Diante deste cenário foram avaliadas as seguintes tecnologias:

- Tecnologia 1) *Software* de proteção de dados
- Tecnologia 2) Servidor de Armazenamento de alta performance
- Tecnologia 3) *Appliances* de Armazenamento de alta densidade
- Tecnologia 4) Armazenamento em Bloco em *Storages*
- Tecnologia 5) *Backup* em fita LTO

#### 2.5.4. ANÁLISE COMPARATIVA DAS SOLUÇÕES

**AT:** Atende, **N AT:** Não Atende, **N AP:** Não se Aplica, **V:** Viável, **I:** Inviável

Requisito	Tecnologia 1	Tecnologia 2	Tecnologia 3	Tecnologia 4	Tecnologia 5
Escalabilidade e Alta Disponibilidade	AT	AT	AT	AT	AT
Armazenamento em Disco de Alta Performance	AT	AT	AT	N AT	N AT
Armazenamento em Disco de Alta Densidade	AT	AT	AT	N AT	N AT
Capacitação Técnica	AT	AT	AT	AT	AT
Atendimento à Legislação vigente	AT	AT	AT	AT	AT
Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo <b>ePing</b>	N AP	N AP	N AP	N AP	N AP
Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo <b>eMag</b>	N AP	N AP	N AP	N AP	N AP
Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo <b>ePWG</b>	N AP	N AP	N AP	N AP	N AP
Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo <b>MoreqJus</b>	N AP	N AP	N AP	N AP	N AP
Se aplicável ser aderente às orientações, premissas e especificações técnicas e funcionais do <b>e-ARQ Brasil</b>	N AP	N AP	N AP	N AP	N AP

<b>Requisito</b>	<b>Tecnologia 1</b>	<b>Tecnologia 2</b>	<b>Tecnologia 3</b>	<b>Tecnologia 4</b>	<b>Tecnologia 5</b>
Se aplicável ser aderente às regulamentações da <b>ICP-Brasil</b> .	N AP	N AP	N AP	N AP	N AP
Entrega Integral e Testes	AT	AT	AT	AT	AT
Técnico Residente Especializado	AT	AT	AT	AT	AT
Comprovação de Expertise	AT	AT	AT	AT	AT
Regras de formação de equipes de operação	N AP	N AP	N AP	N AP	N AP
Garantia e Subscrição de Longo Prazo	AT	AT	AT	AT	AT
Migração Segura dos Jobs	AT	AT	AT	AT	AT
Atualizações e Patches	AT	AT	AT	AT	AT
Alinhamento Estratégico	AT	AT	AT	AT	AT
Solução Abrangente de Proteção de Dados (Backup e Restore)	AT	AT	AT	AT	AT
Metodologia Ágil e Documentação	AT	AT	AT	AT	AT
Alta Disponibilidade e Redundância	AT	AT	AT	AT	AT
Proteção contra Ameaças e Integridade dos Dados	AT	AT	AT	AT	AT
Proteção contra Ransomware e Segurança Cibernética	AT	AT	AT	AT	AT
Sustentabilidade e Eficiência Energética	AT	AT	AT	AT	AT
Eficiência Energética e Descarte Sustentável	AT	AT	AT	AT	AT
SLA de Alta Disponibilidade	AT	AT	AT	AT	AT
Gerenciamento Técnico e Sustentação 24x7	AT	AT	AT	AT	AT
Horas Técnicas Especializadas Sob Demanda	AT	AT	AT	AT	AT
Compatibilidade e Integração	AT	AT	AT	AT	AT
Estratégia de Proteção 3-2-1	AT	AT	AT	AT	AT
Compatibilidade com Ambientes Modernos (K8s, Nuvem e Virtualização)	AT	AT	AT	AT	AT
Instant Recovery	AT	AT	AT	AT	AT
Prazo de Implantação	AT	AT	AT	AT	AT
<b>Resultado da Análise</b>	<b>V</b>	<b>V</b>	<b>V</b>	<b>I</b>	<b>I</b>

## 2.5.4.2. Soluções Viáveis

### 2.5.4.2.1. Tecnologia 1- *Software* de proteção de dados

2.5.4.2.1.1. Este é o componente essencial de qualquer solução de proteção de dados, atuando como o orquestrador de todos os equipamentos que serão incluídos nesta contratação, ou que foram contratados no expediente 0107633-28.2022.8.16.6000. A Tecnologia 1 foi considerada viável após análise comparativa, atendendo integralmente aos requisitos estratégicos, técnicos e legais definidos pelo Tribunal de Justiça do Estado do Paraná (TJ/PR), apresentando características robustas que garantem alta disponibilidade, escalabilidade e desempenho superior, essenciais para suportar o crescimento contínuo da volumetria de dados e assegurar a continuidade dos serviços judiciais. Além disso, a Tecnologia 1 atende plenamente às necessidades identificadas no Estudo Técnico Preliminar, oferecendo uma solução abrangente para proteção de dados, alinhada às diretrizes estratégicas do TJ/PR e às normas nacionais, contribuindo para a mitigação de riscos, a conformidade regulatória e a eficiência operacional, garantindo segurança, confiabilidade e sustentabilidade ao longo do ciclo contratual.

### 2.5.4.2.2. Tecnologia 2 - Servidor de Armazenamento de alta performance

2.5.4.2.2.1. A Tecnologia 2 foi classificada como viável após avaliação criteriosa, atendendo integralmente aos requisitos técnicos, legais e estratégicos definidos pelo Tribunal de

Justiça do Estado do Paraná (TJ/PR), destacando-se pela robustez, escalabilidade e aderência às melhores práticas de proteção de dados, o que garante alta confiabilidade e segurança para os serviços judiciais. Além disso, a Tecnologia 2 atende plenamente às necessidades identificadas no Estudo Técnico Preliminar, oferecendo uma solução abrangente e segura para proteção de dados, cuja adoção contribui para a mitigação de riscos, conformidade regulatória e eficiência operacional, assegurando alta disponibilidade, escalabilidade e sustentabilidade ao longo do contrato.

#### 2.5.4.2.3. Tecnologia 3 - *Appliances* de Armazenamento de alta densidade

2.5.4.2.3.1. Os *appliances* são dispositivos de armazenamento projetados especificamente para soluções de backup, oferecendo recursos avançados de segurança, alta disponibilidade e desempenho superior, tanto na gravação quanto na recuperação dos dados. A Tecnologia 3 foi considerada viável após análise comparativa, atendendo integralmente aos requisitos estratégicos, técnicos e legais definidos pelo Tribunal de Justiça do Estado do Paraná (TJ/PR), apresentando características robustas que garantem alta disponibilidade, escalabilidade e desempenho superior, essenciais para suportar o crescimento contínuo da volumetria de dados e assegurar a continuidade dos serviços judiciais. Além disso, a Tecnologia 3 atende plenamente às necessidades identificadas no Estudo Técnico Preliminar, oferecendo uma solução abrangente e segura para proteção de dados, cuja adoção contribui para a mitigação de riscos, conformidade regulatória e eficiência operacional, garantindo alta disponibilidade, escalabilidade e sustentabilidade ao longo do contrato.

### 2.5.5. JUSTIFICATIVA DA CONTRATAÇÃO COM VIGÊNCIA DE 60 MESES

2.5.5.1. A contratação da solução de proteção de dados com vigência de 60 meses revela-se mais adequada e vantajosa em relação a uma contratação limitada a 12 meses, considerando a natureza estratégica, contínua e crítica do serviço para a Administração Pública. Trata-se de solução que sustenta diretamente a continuidade dos serviços judiciais e administrativos considerados essenciais, a segurança da informação e a proteção de dados pessoais, de modo que a interrupção do suporte, da subscrição de software ou da garantia dos equipamentos implicaria riscos elevados à disponibilidade, à integridade e à recuperabilidade das informações institucionais. Nesse contexto, a adoção de um prazo contratual reduzido mostrar-se-ia incompatível com o princípio da continuidade do serviço público e com as diretrizes de segurança e governança de TIC aplicáveis ao Poder Judiciário.

2.5.5.2. Sob a ótica da economicidade, a vigência de 60 meses permite a adequada diluição, ao longo do ciclo de vida da solução, dos custos de implantação, licenciamento, migração de *jobs*, capacitação, suporte especializado e gerenciamento técnico, evitando a repetição periódica de despesas iniciais que seriam inevitáveis em contratações anuais sucessivas. A contratação de curto prazo tende a gerar retrabalho administrativo, perda de economia de escala e elevação do custo total da solução ao longo do tempo, em desacordo com as boas práticas de planejamento e com a análise do custo total de propriedade recomendadas pelos órgãos de controle como o Tribunal de Contas da União (TCU) e o Tribunal de Contas do Estado do Paraná (TCE/PR).

2.5.5.3. A contratação por prazo mais amplo também contribui de forma significativa para a mitigação de riscos operacionais, jurídicos e de mercado, ao reduzir a dependência de processos licitatórios frequentes para a manutenção de um serviço essencial, bem como a exposição a variações de preços, alterações abruptas em modelos de licenciamento ou descontinuidade de suporte por parte de fabricantes. Além disso, assegura maior estabilidade operacional, preserva o conhecimento acumulado sobre a solução e fortalece a governança contratual, aspectos reiteradamente valorizados em entendimentos do TCU e do TCE/PR no âmbito das contratações de TIC.

Por fim, a definição da vigência contratual de 60 meses encontra respaldo na legislação vigente, em especial na Lei nº 14.133/2021, e mostra-se plenamente alinhada ao planejamento estratégico institucional, ao Plano Diretor de TIC e às diretrizes nacionais de segurança cibernética do Poder Judiciário. Dessa forma, a opção por esse prazo não apenas atende aos princípios da eficiência, da economicidade e do interesse público, como também se apresenta como solução tecnicamente consistente e juridicamente segura para assegurar a continuidade, a confiabilidade e a sustentabilidade da solução de proteção de dados ao longo do tempo.

## 2.6. RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA

2.6.1. Para estimar a volumetria necessária à implementação da solução de proteção de dados, foram realizadas inicialmente dez reuniões com as equipes responsáveis pelos *jobs* de backup ativos, conforme registrado no “Relatório de Reuniões de Levantamento para o Plano de Backup” (SEI nº 12695304). Nessas reuniões, as equipes foram incumbidas de validar os *jobs* existentes, incluir novas demandas de backup e atualizar o volume de dados a ser protegido, resultando na elaboração da “Planilha Plano de Backup” (SEI nº 12695323).

2.6.2. Os dados constantes dessa planilha, aliados às premissas e informações obtidas dos serviços Microsoft 365, foram compartilhados, de forma anonimizada, com três parceiros/fabricantes. Contudo, apenas um fabricante apresentou resposta, fornecendo a estimativa de volumetria necessária para atender à demanda do Tribunal de Justiça do Estado do Paraná, conforme disposto no “Relatório Estimado de Processamento e Volumetria” (SEI nº 12695348).

2.6.3. Com base nessas informações, seguem as estimativas das quantidades e serviços a serem adquiridas:

- Microsoft 365: 16.000 contas;
- Kubernetes/Tanzu: 50 *worker nodes*;
- Máquinas Virtuais: 800 VMs;
- Hosts: 148 servidores;
- Área de Armazenamento NAS: 700 TB;
- Servidores de Sustentação do Software de Proteção de Dados e Área de armazenamento de alta performance;
- Área de armazenamento de alta densidade *appliances*;
- Permitir *Instant Recovery* de, no mínimo, 60 VMs simultaneamente;
- Migração de 150 *Jobs* de backup;
- Garantia, suporte e subscrição por, no mínimo, 60 meses;
- Capacitação no *software* de proteção de dados e *Appliances*
- Serviço de gerenciamento técnico e sustentação da solução;
- Horas técnicas especializadas;

### 2.6.4. DIMENSIONAMENTO DA SOLUÇÃO

RECURSO	CAPACIDADE/QUANTIDADE
Servidores de Sustentação do Software de Proteção de Dados e Área de armazenamento de alta performance	400 TB
Área de armazenamento de alta densidade <i>appliances</i> ;	1.000 TB
Área de Armazenamento NAS	700 TB
Contas Microsoft 365 para backup	16.000
Máquinas virtuais	800
Nós Kubernetes ( <i>workernodes</i> )	50
Servidores físicos ( <i>hosts</i> )	148
Instant Recovery de VMs Simultaneamente	60
Capacitação no <i>software</i> de proteção de dados e <i>Appliances</i>	12
Número de <i>Jobs</i> a serem migrados	150

### 2.6.5. DESCRIÇÃO DA SOLUÇÃO DE TIC COMO UM TODO

2.6.5.1. A solução proposta para o Tribunal de Justiça do Estado do Paraná (TJ/PR) consiste em um conjunto integrado de tecnologias e serviços que asseguram a proteção completa dos dados institucionais, garantindo alta disponibilidade, escalabilidade, segurança e conformidade com as normas legais e estratégicas vigentes.

#### 2.6.5.2. Componentes Tecnológicos:

- **Software de Proteção de Dados:** Plataforma avançada para gerenciamento de backup e restauração, com recursos de deduplicação, criptografia, proteção contra ransomware e integração com ambientes modernos (máquinas virtuais, Kubernetes, nuvem e soluções híbridas). Essa camada é responsável por orquestrar políticas de proteção, monitoramento e recuperação rápida, assegurando a continuidade dos serviços judiciais.
- **Servidor de Armazenamento de alta performance:** Infraestrutura otimizada para operações críticas de backup e restore, garantindo velocidade e confiabilidade na execução dos processos. Ideal para dados de alta rotatividade e sistemas que exigem respostas imediatas.
- **Appliances de Armazenamento de alta densidade:** Equipamentos dedicados para armazenamento massivo, com alta capacidade e eficiência energética, destinados à retenção de longo prazo e à escalabilidade da solução. Essa camada complementa a estratégia de proteção 3-2-1-0, assegurando redundância e resiliência.

#### 2.6.5.3. Serviços Associados:

- **Instalação, Configuração e Migração dos *Jobs*:** A implementação da solução compreenderá todas as etapas necessárias, incluindo a integração com os ambientes existentes e a validação funcional. Além disso, durante a execução dos serviços, será realizada a transferência segura dos *jobs* de backup da solução atual para a nova plataforma, permitindo a análise individual de cada *job*, testes de restauração, a aplicação de boas práticas e a adequada adaptação às características da solução contratada e dos ambientes já existentes.
- **Capacitações e Transferência de Conhecimento:** A contratação de serviços de capacitação e transferência de conhecimento mostra-se indispensável para assegurar a efetiva apropriação, pela equipe técnica do Tribunal, da solução de proteção de dados a ser implantada, considerando sua elevada complexidade tecnológica, a criticidade do serviço e a inexistência, na estrutura organizacional, de cargo específico dedicado à especialidade de backup e proteção de dados. Conforme evidenciado nos documentos anexados, a solução abrange múltiplas tecnologias — incluindo ambientes virtualizados, contêineres, armazenamento de alta performance e alta densidade, além de integração com serviços em nuvem — cuja correta operação, fiscalização e evolução dependem de conhecimento técnico aprofundado. A capacitação formal e estruturada permite que os servidores compreendam a arquitetura implementada, as políticas de proteção, os mecanismos de segurança, os procedimentos de restauração e os indicadores de desempenho contratual, fortalecendo a governança de TIC, a fiscalização do contrato e a mitigação de riscos de dependência excessiva da contratada. Ademais, a transferência de conhecimento está alinhada às boas práticas de contratações públicas de TIC, ao princípio da eficiência e às diretrizes de segurança da informação do Poder Judiciário, garantindo continuidade operacional, preservação do conhecimento institucional e maior sustentabilidade da solução ao longo de sua vigência contratual.
- **Gerenciamento Técnico e Sustentação:** A contratação do serviço de Gerenciamento Técnico e Sustentação da solução de proteção de dados é imprescindível para garantir a operação contínua, segura e eficiente de um ambiente tecnológico classificado como crítico e estratégico para o Tribunal. A solução envolve múltiplas camadas de software, hardware especializado, integração com ambientes virtualizados, contêineres, serviços em nuvem e políticas avançadas de segurança da informação, demandando monitoramento permanente, atuação proativa na prevenção e resolução de incidentes e aplicação contínua de atualizações e boas práticas recomendadas pelos fabricantes. Considerando que a estrutura organizacional não dispõe de cargo específico voltado à especialidade de backup e proteção de dados, e que a equipe interna já

acumula atribuições relacionadas a outros ativos de TIC, o gerenciamento técnico especializado assegura níveis de serviço compatíveis com a criticidade da solução, reduz o risco de falhas operacionais, indisponibilidades ou perda de dados e fortalece a segregação de responsabilidades. Ademais, o serviço de sustentação contínua, com atendimento e indicadores de desempenho definidos, está alinhado às diretrizes de governança, continuidade do serviço público e mitigação de riscos preconizadas pela legislação vigente e pelas boas práticas de contratações de TIC, garantindo maior estabilidade operacional, previsibilidade na execução contratual e efetiva proteção das informações institucionais ao longo de toda a vigência da contratação.

- **Horas Técnicas Especializadas sob Demanda:** A contratação de Horas Técnicas Especializadas sob Demanda é justificada pela necessidade de conferir flexibilidade, capacidade de resposta e segurança técnica à operação e à evolução da solução de proteção de dados. Considerando a complexidade do ambiente tecnológico contemplado — que envolve integração com múltiplas plataformas, ambientes virtualizados, contêineres, serviços em nuvem e requisitos rigorosos de segurança da informação — é previsível a ocorrência de demandas extraordinárias não integralmente mensuráveis na fase de planejamento, tais como ajustes avançados de configuração, suporte a incidentes complexos, expansões de escopo, adequações a novas normativas, auditorias técnicas, testes de recuperação de desastres ou apoio especializado em situações críticas. A previsão contratual de horas técnicas sob demanda permite o atendimento célere e qualificado dessas necessidades sem a interrupção dos serviços essenciais nem a instauração de novos e morosos processos licitatórios, reduzindo riscos operacionais e assegurando a continuidade do negócio. Ademais, esse modelo fortalece a governança contratual, promove maior eficiência na gestão da solução e está alinhado às boas práticas de contratações de TIC no setor público, ao possibilitar que a Administração disponha de expertise especializada de forma controlada, transparente e economicamente racional ao longo da vigência contratual.

#### 2.6.5.4. Benefícios da Solução Integrada:

- **Segurança e Conformidade:** Atende às exigências da Lei 14.133/2021, Resolução CNJ 468/2022 e Guia de Contratações de TI do CNJ.
- **Alta Disponibilidade e Resiliência:** Reduz riscos de indisponibilidade e perda de dados, garantindo continuidade operacional.
- **Escalabilidade e Sustentabilidade:** Preparada para crescimento futuro e alinhada às práticas ambientais.
- **Eficiência Operacional:** Integração completa entre software, hardware e serviços, com suporte especializado e SLA rigoroso.

2.6.5.5. Essa arquitetura integrada assegura que o TJ/PR disponha de uma solução moderna, robusta e aderente às melhores práticas do setor público, garantindo proteção, governança e evolução tecnológica ao longo do ciclo contratual.

### 3. REQUISITOS DA CONTRATAÇÃO

Tipo	Requisito	Descrição	Justificativa
	Escalabilidade e Alta Disponibilidade	A solução deve suportar crescimento da volumetria e operar em ambos os datacenters, garantindo continuidade em caso de falhas.	Atende à necessidade de alta disponibilidade e expansão futura, reduzindo riscos de indisponibilidade.

Tipo	Requisito	Descrição	Justificativa
Capacidade, Configuração e Desempenho	Armazenamento em Disco de Alta Performance	Fornecimento de Servidores de backup com discos SSD conectados via NVME, com a capacidade mínima a ser exigida em cada equipamento, sem considerar deduplicação/compactação.	Dispositivos dedicados oferecem segurança, resiliência e desempenho superiores a servidores comuns. O uso de SSD/NVME é essencial para garantir janelas de backup curtas e recuperação rápida (Instant Recovery).
	Armazenamento em Disco de Alta Densidade	Fornecimento de Appliances de backup com a aplicação de recursos de deduplicação e compactação.	Dispositivos dedicados que oferecem alta retenção de dados. Permitindo o armazenamento histórico por um longo período.
Capacitação e Transferência de Conhecimento	Capacitação Técnica	Disponibilização de capacitação completa para a equipe do Tribunal sobre a operação e funcionalidades da solução.	Essencial para que a equipe de fiscalização e a gestão interna compreendam a arquitetura implementada e possam auditar a qualidade do serviço prestado pela contratada.
Conformidade Técnica ou Requisitos Legais	Atendimento à Legislação vigente	· Lei Federal nº 14.133/2021;· Decreto Estadual do Estado do Paraná nº 10.086/2022;· Resolução do Conselho Nacional de Justiça nº 468/2022;· Lei Geral de Proteção de Dados nº 13.709/2018;· Lei Federal nº 9.609/1998 (Lei de Proteção da Propriedade Intelectual de Programa de Computador);· Decreto Judiciário TJPR nº 269/2022 e· Instrução Normativa TJPR nº 196/2024· Resolução CNJ 370/2021	Garante legalidade e conformidade, evitando nulidades e responsabilizações.
Conformidade	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo ePing	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.
	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo eMag	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.
	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo ePWG	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.

<b>Técnica</b>	<b>Requisito</b>	<b>Descrição</b>	<b>Justificativa</b>
Requisitos Legais	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo MoreqJus	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.
	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.
	Atendimento às Normas CNJ e do Governo	Se aplicável ser aderente às regulamentações da ICP-Brasil.	Garante atendimento a requisitos normativos e conformidade, evitando soluções fora do padrão definido.
Entrega	Entrega Integral e Testes	Todos os componentes (software, appliances, serviços) devem ser entregues e testados antes da aceitação definitiva.	Garante conformidade com especificações e funcionamento adequado, evitando falhas pós-implantação.
Experiência Profissional	Técnico Residente Especializado	Disponibilização do serviço de operação por meio de um profissional residente, com conhecimento em todas as tecnologias contratadas.	Garante suporte imediato e gestão eficiente da solução, reduzindo tempo de resolução de problemas.
Experiência Profissional Formação de Equipe	Comprovação de Expertise	Fornecedor deve comprovar experiência em projetos similares.	Reduz riscos de contratação de fornecedores sem expertise, garantindo qualidade na entrega.
	Regras de formação de equipes de operação	Por tratar-se de solução de proteção de dados com o fornecimento de serviço de operação e não de postos de trabalho, não há necessidade do apontamento de requisito de formação de equipe.	
Garantia	Garantia e Subscrição de Longo Prazo	Garantia, suporte técnico do fabricante e subscrição de software/hardware por, no mínimo, 60 meses para todos os itens.	Equipamentos e softwares com suporte vencido representam risco de segurança (falta de patches). O prazo de 60 meses garante longevidade ao investimento e estabilidade operacional.
Implantação	Migração Segura dos Jobs	Deve incluir migração completa dos jobs de backup, com validação e testes de restauração.	Minimiza riscos de perda de dados e assegura continuidade operacional durante a transição.
Manutenção e Atualização	Atualizações e Patches	A solução deve incluir atualizações regulares de software e firmware, sem custo adicional, durante todo o contrato.	Mantém segurança e desempenho, evitando vulnerabilidades e obsolescência tecnológica.



<b>Tipo</b>	<b>Requisito</b>	<b>Descrição</b>	<b>Justificativa</b>
Negócio	Alinhamento Estratégico	A solução deve estar alinhada ao Planejamento Estratégico do TJPR e ao PDTIC, garantindo aderência às metas institucionais e objetivos estratégicos.	Evita investimentos desalinhados e assegura que a contratação contribua para os objetivos do Judiciário.
NegócioProjeto e Metodologia de Trabalho	Solução Abrangente de Proteção de Dados (Backup e Restore)	A solução deve fornecer proteção completa de dados, indo além do backup tradicional para incluir recuperação de desastres, prevenção contra perda, corrupção e roubo de informações, garantindo a continuidade dos serviços essenciais do Tribunal.	A simples cópia de segurança não é mais suficiente frente às ameaças atuais. Uma solução abrangente é vital para evitar perdas financeiras severas e garantir a continuidade operacional, especialmente considerando que a solução atual não suporta recuperação de desastres adequada.
	Metodologia Ágil e Documentação	A implantação deve seguir boas práticas (PMI, ITIL ou equivalente), com cronograma detalhado e entrega de documentação completa da arquitetura.	Facilita gestão do projeto, controle de riscos e manutenção futura, garantindo rastreabilidade.
Projeto e Metodologia de TrabalhoSegurança	Alta Disponibilidade e Redundância	A solução deve operar em ambos os datacenters do Tribunal. Em caso de queda de um datacenter, o outro deve assumir integralmente a sustentação e recuperação dos dados.	A solução atual não possui alta disponibilidade, criando risco de perda de dados se um datacenter falhar. A redundância é crítica para a continuidade dos serviços judiciais e administrativos.
	Proteção contra Ameaças e Integridade dos Dados	A solução deve garantir mecanismos robustos de segurança, incluindo criptografia, autenticação forte, controle de acesso e auditoria detalhada.	A integridade e confidencialidade dos dados do TJ/PR são fundamentais para a continuidade dos serviços judiciais.
SegurançaSociais, Ambientais e Culturais	Proteção contra Ransomware e Segurança Cibernética	A solução deve incluir mecanismos de proteção contra-ataques cibernéticos, criptografia e garantir a integridade dos dados, alinhada à Estratégia Nacional de Segurança Cibernética (ENSEC-PJ).	O backup é a última linha de defesa. Com o aumento de ameaças como ransomware, é indispensável que a solução não apenas copie, mas proteja os dados contra corrupção e sequestro, garantindo conformidade com a LGPD.
	Sustentabilidade e Eficiência Energética	Equipamentos devem possuir certificações ambientais (Energy Star, ISO 14001) e fornecedores devem adotar práticas sustentáveis, incluindo logística reversa.	Reduz impactos ambientais e cumpre princípios da Administração Pública (art. 5º, Lei 14.133/2021).

Tipo	Requisito	Descrição	Justificativa
Sociais, Ambientais e Culturais Suporte, SLA e ANS	Eficiência Energética e Descarte Sustentável	Os equipamentos devem possuir certificações de eficiência energética e o fornecedor deve garantir o descarte adequado (logística reversa) se aplicável ao fim da vida útil.	O consumo de energia e a geração de resíduos eletrônicos são impactos ambientais diretos desta contratação. Mitigar esses efeitos é uma obrigação legal e social da administração pública.
	SLA de Alta Disponibilidade	Atendimento 24x7, com tempo máximo de resposta de 1 hora para incidentes críticos e penalidades por descumprimento.	Assegura níveis de serviço compatíveis com criticidade da solução, garantindo continuidade e mitigação de riscos.
Suporte, SLA e ANS Tecnológico	Gerenciamento Técnico e Sustentação 24x7	Serviço de gerenciamento técnico e sustentação operacional ininterrupto (24x7x365), com atendimento presencial em horário regimental.	O TJPR não possui cargo de "Analista de Backup". A equipe atual acumula funções e não tem especialização suficiente. A terceirização da operação é necessária para garantir monitoramento proativo e resolução rápida de incidentes.
	Horas Técnicas Especializadas Sob Demanda	Disponibilização de até 1.000 horas de consultoria técnica especializada para melhorias, novas funcionalidades e apoio em crises.	Permite flexibilidade para lidar com demandas imprevistas, atualizações complexas ou expansões do ambiente sem a necessidade de novos processos licitatórios morosos.
	Compatibilidade e Integração	Deve integrar-se aos ambientes existentes (máquinas virtuais, Kubernetes, Microsoft 365, Teams) e seguir arquitetura 3-2-1-0 de backup.	Evita retrabalho e garante interoperabilidade com sistemas atuais, assegurando eficiência operacional.
	Estratégia de Proteção 3-2-1-0	A arquitetura deve seguir o conceito 3-2-1-0: manter três cópias dos dados, em dois tipos diferentes de mídia (disco/nuvem), com uma cópia fora do local físico principal (offsite).	Esta é uma prática recomendada mundialmente por especialistas em segurança para garantir resiliência, mitigando riscos de falhas de hardware, erros humanos, ataques de ransomware e desastres naturais.

Tipo	Requisito	Descrição	Justificativa
TecnológicoTemporal	Compatibilidade com Ambientes Modernos (K8s, Nuvem e Virtualização)	Suporte nativo a Kubernetes/Tanzu, Microsoft 365 (Teams, SharePoint, Exchange), Máquinas Virtuais VMware, e bancos de dados (PostgreSQL, SQL Server, MySQL, Sybase).	A infraestrutura do TJPR evoluiu para uso de contêineres e nuvem, tecnologias que a solução legada atual não suporta, deixando dados críticos desses ambientes vulneráveis e sem backup adequado.
	Instant Recovery	Capacidade de realizar a recuperação instantânea (Instant Recovery)	Em caso de desastre ou falha crítica de servidores, o tempo de recuperação (RTO) precisa ser mínimo para não paralisar o Tribunal. Esta funcionalidade permite subir os serviços diretamente do backup.
	Prazo de Implantação	A implantação completa da solução deve ocorrer em até 270 dias após assinatura do contrato, incluindo migração dos jobs em até 30 dias após ativação.	Reduz riscos de indisponibilidade e garante continuidade dos serviços essenciais de TIC.

#### 4. MODELO DE EXECUÇÃO DO OBJETO

##### 4.1. DINÂMICA DA EXECUÇÃO

FASE	ITEM	DESCRIÇÃO	QUANDO OCORRE?
1	Todos	Assinatura do contrato entre as partes.	Após a homologação do certame
2	Todos	Reunião inicial (kick-off) com a CONTRATADA para esclarecimentos relativos a questões operacionais, administrativas e de gestão de contrato.	Em até 7 (sete) dias corridos após a assinatura do contrato.
3	1	Entrega do item 1 pela CONTRATADA.	Em até 30 (trinta) dias corridos após a assinatura do contrato, ou seja, fase 1.
4	1	Instalação, configuração e implantação do item 1 pela CONTRATADA	Em até 20 (vinte) dias corridos após conclusão da fase 3.
5	1	Emissão pela CONTRATANTE do Termo de Recebimento Definitivo 1 (TRD1).	Em até 20 (vinte) dias corridos após conclusão da fase 4, relacionado ao item 1.
6	1	Pedido de pagamento.	Após conclusão da fase 5.
7	2 e 3	Entrega dos itens 2 e 3 pela CONTRATADA.	Em até 150 (cento e cinquenta) dias corridos após assinatura do contrato, ou seja, fase 1.
8	4	Instalação, configuração e implantação da solução e entrega pela CONTRATADA do Relatório final de implementação.	Em até 20 (vinte) dias corridos após conclusão da fase 7.
9	2 e 3	Emissão pela CONTRATANTE do Termo de Recebimento Definitivo 2 (TRD2).	Em até 30 (trinta) dias corridos após conclusão da fase 8, relacionado aos itens 2 e 3.
10	2 e 3	Pedido de pagamento.	Após conclusão da fase 5

FASE	ITEM	DESCRIÇÃO	QUANDO OCORRE?
11	4, 5 e 6	Capacitação e Migração do Jobs, bem como entrega pela CONTRATADA do plano de backup contendo os jobs migrados e testados.	Em até 30 (trinta) dias corridos após conclusão da fase 8.
12	4, 5 e 6	Emissão pela CONTRATANTE do Termo de Recebimento Definitivo 3 (TRD3).	Em até 30 (trinta) dias corridos após conclusão da fase 11, relacionado aos itens 4, 5 e 6.
13	4, 5 e 6	Pedido de pagamento.	Após conclusão da fase 12.
14	7	Execução do serviço de Gerenciamento Técnico e Sustentação da Solução de Proteção de Dados.	Após a conclusão da fase 3, mediante solicitação da CONTRATANTE.
15	7	Emissão pela CONTRATADA do Relatório Gerencial de Atividades com o cálculo do índice de chamados resolvidos dentro do prazo.	Mensalmente durante a execução da fase 14.
16	7	Pedidos de pagamento mensal.	Após conclusão da fase 15.
17	7	Realização pela CONTRATANTE do Atesto da fatura mensal em relação a prestação de serviço da fase 10.	Conforme legislação vigente, após execução da fase 15 com a inclusão do Relatório Gerencial de Atividades.
18	8	Abertura da Ordem de Serviço pela CONTRATANTE para atividades sob demanda com Horas técnicas especializadas.	Sempre que solicitado.
19	8	Emissão pela CONTRATANTE do Termo de Recebimento Definitivo relativo a horas técnicas sob demanda.	Em até 30 (trinta) dias corridos após conclusão do serviço.
20	8	Pedidos de pagamento atividades sob demanda.	Após conclusão da fase 19.

4.1.2. Realizar-se-á reunião inicial (*kick-off*) para planejamento e alinhamento, visando identificar expectativas, nivelar entendimentos sobre as condições estabelecidas no Contrato, no Edital e seus Anexos, bem como esclarecer eventuais dúvidas referentes à execução do serviço. Participarão obrigatoriamente desta reunião: o Gestor do Contrato, os Fiscais Operacionais e a CONTRATADA. A reunião ocorrerá na modalidade remota, conforme agendamento a ser determinado pelo Gestor do Contrato, ocasião em que a contratada deverá apresentar formalmente seu PREPOSTO.

4.1.3. A execução do objeto do presente Contrato será de forma indireta, sob o regime de empreitada por preço global, em conformidade com o disposto no art. 490 da Decreto Estadual nº 10.086/2022.

4.1.4. Considerando que o valor da contratação ultrapassará a quantia de R\$ 5.000.000,00 (cinco milhões de reais), a CONTRATADA deverá entregar o Formulário de Análise de Perfil das Contratadas do Tribunal de Justiça do Estado do Paraná no prazo de até 30 (trinta) dias corridos contados após a assinatura do contrato, sob pena de aplicação das sanções previstas neste Termo de Referência, conforme Decreto Judiciário nº 62/2026. A solicitação de preenchimento de formulário será enviada à contratada pelo gestor do contrato, por meio de link, em até 5 (cinco) dias úteis após a assinatura do instrumento contratual.

## 4.2. VIGÊNCIA CONTRATUAL

A vigência do contrato será de 60 (sessenta) meses contados da emissão do Termo de Recebimento Definitivo 3 (TRD3).

## 4.3. INSTRUMENTOS DE SOLICITAÇÃO DO(S) SERVIÇO(S)

4.3.1. Os instrumentos de solicitação dos serviços deverão observar todos os requisitos técnicos estabelecidos no presente Termo de Referência e seus Anexos, com especial atenção às especificações constantes do Anexo 04.

4.3.2. Todas as interações entre as partes serão formalmente documentadas e registradas no processo de fiscalização contratual, observando-se as normas de gestão documental

aplicáveis, de modo a assegurar a rastreabilidade dos fatos ocorridos durante a vigência do contrato e a preservação do histórico de execução, especialmente para fins de prestação de contas aos órgãos de controle interno e externo.

4.3.3. Toda a comunicação entre o CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação, em consonância com o item 4.5 Mecanismos Formais de Comunicação.

4.3.4. A Ordem de Serviço (OS) é o ato administrativo que autoriza cada parcela do serviço contratado. Para garantir rastreabilidade, eficiência fiscalizatória e pleno atendimento à Lei 14.133/2021, toda OS deverá conter no mínimo: (i) Identificação da OS, (ii) Identificação da Contratada, (iii) Objeto e Especificação do Serviço, (iv) Estimativa de Esforço ou Quantitativos, (v) Local, Prazos e Janelas de Execução, (vi) Recursos Financeiros, (vii) Critérios de Aceitação e Indicadores, (viii) Responsáveis pelo Ciclo da OS.

#### **4.4. MONITORAMENTO DA EXECUÇÃO**

4.4.1. A CONTRATADA deverá manter PREPOSTO para representá-la durante o fornecimento dos produtos e a prestação dos serviços ora tratados, desde que aceito pelo CONTRATANTE.

4.4.2. Ao PREPOSTO cabe, por exemplo, a responsabilidade pelas seguintes atividades:

- Executar os procedimentos administrativos referentes aos profissionais da CONTRATADA alocados para execução dos serviços contratados, tais como acompanhar e controlar a frequência, controlar afastamentos, (seja por motivo de férias, atestados médicos ou outros afastamentos programados ou não) e, ainda, responder por qualquer assunto administrativo e de recursos humanos entre os colaboradores da CONTRATADA e as operações da empresa;
- Responder por todas as questões administrativas da CONTRATADA junto ao CONTRATANTE, bem como, receber e responder ofícios e solicitações administrativas, controlar o uso de recursos computacionais e de comunicações pelos colaboradores da CONTRATADA, manter atualizados os requisitos técnicos e habilitatórios necessários à execução do contrato;
- Assegurar que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais envolvidos na prestação dos serviços com vistas à correta execução dos serviços contratados;
- Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;
- Formalizar junto a CONTRATANTE eventos de afastamento ou substituição de colaboradores diretamente envolvidos na execução dos serviços; e
- Desenvolver outras atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos, quando solicitado.

4.4.3. As decisões e providências que ultrapassarem a competência do PREPOSTO deverão ser solicitadas aos seus superiores em tempo hábil para adoção das medidas convenientes.

4.4.4. O PREPOSTO não poderá acumular papel, cobrir requisitos de qualificação técnica ou ser substituto de profissionais, na operação técnica da prestação dos serviços contratados.

4.4.5. Ao CONTRATANTE é reservado o direito de efetuar diligência, a qualquer tempo, quanto aos documentos exigidos neste Termo de Referência e em seus Anexos.

4.4.6. A existência e a atuação da fiscalização em nada restringem a responsabilidade, única, integral e exclusiva da CONTRATADA, no que concerne à execução do objeto contratado.

4.4.7. Todos os documentos apresentados estarão sujeitos à diligência da contratante para fins de confirmação das informações prestadas.

4.4.8. O acompanhamento da contratação deverá atender a todos os requisitos especificados neste Termo de Referência e em seus Anexos.

#### **4.5. MECANISMOS FORMAIS DE COMUNICAÇÃO**

4.5.1. Toda a comunicação entre o Contratante e a Contratada deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação:

- **Documento:** ofícios, e-mails, relatórios e outros correlatos que possam ficar registrados;
- **Emissor:** gestor do contrato, fiscal técnico do contrato, fiscal requisitante do contrato e fiscal administrativo do contrato;
- **Destinatário:** preposto da contratada e representante legal da Contratada;
- **Meio:** Os documentos poderão ser entregues pessoalmente, mediante recibo, pelos Correios, ou meio eletrônico;
- **Periodicidade:** Sempre que se fizer necessário à comunicação com a Contratada.

#### 4.6. TRANSFERÊNCIA DE CONHECIMENTO

4.6.1. No que diz respeito à execução de horas técnicas especializadas sob demanda, durante toda a vigência do contrato, poderá haver transferência de conhecimento, capacitações, consultorias e auditorias. Esses serviços serão faturados conforme as requisições estabelecidas em Ordem de Serviço.

4.6.2. A CONTRATADA deverá se comprometer a habilitar a equipe de técnicos do CONTRATANTE ou outra por ele indicada no uso de eventuais soluções desenvolvidas e implantadas ou nos produtos fornecidos dentro do escopo do CONTRATO, repassando todo o conhecimento necessário para tal, com vistas a mitigar riscos de descontinuidade dos serviços e de dependência técnica.

4.6.3. A CONTRATADA deverá realizar, no ambiente do TJPR ou em laboratório virtual dedicado, capacitação formato hands-on cobrindo: instalação, administração, automação de rotinas, restauração e troubleshooting da solução.

4.6.4. A capacitação deverá ser realizada com acesso individual ou compartilhado à instância da ferramenta, permitindo que os participantes executem operações reais em ambiente controlado.

4.6.5. O conteúdo deverá ser voltado à aplicação direta do conhecimento técnico, com demonstrações práticas seguidas de atividades conduzidas pelos próprios participantes.

4.6.6. Todo material deverá ser fornecido em formato aberto e editável (ODF, Markdown ou equivalente) e arquivado no repositório oficial do TJPR.

4.6.7. Scripts, playbooks Ansible, manuais de API (S3, REST, CLI) e diagramas fazem parte obrigatória dos entregáveis.

4.6.8. Demais especificações referentes a capacitação constam no Anexo 07 – Requisitos Técnicos.

#### 4.7. NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

4.7.1. A fiscalização, exercida no interesse do CONTRATANTE e com vistas à satisfação do interesse público, não exime nem reduz a responsabilidade da CONTRATADA por qualquer dano causado ao CONTRATANTE ou a terceiros.

4.7.2. O CONTRATANTE poderá alterar os procedimentos de avaliação durante a execução do contrato, desde que o novo sistema seja mais eficiente e não cause prejuízos à CONTRATADA, mediante comunicação prévia.

4.7.3. A medição da qualidade dos serviços será realizada pelo Fiscal Técnico, Fiscal Administrativo e Gestor do Contrato, utilizando um sistema de percentual de execução, reiniciado a cada mês, cujo resultado determinará o valor a ser pago no período avaliado.

4.7.4. As situações abrangidas por este instrumento se referem aos aspectos cotidianos da execução do Contrato, sem isentar a CONTRATADA de suas demais responsabilidades ou sanções previstas em lei.

4.7.5. Devido ao modelo de negócio dos softwares de proteção de dados oferecidos no Brasil, o Tempo de Solução não será considerado para o Item 1. Para esse item, será utilizado o SLA de Atendimento, o qual está definido nos requisitos técnicos do item.

4.7.6. Chamados que demandem a intervenção do fabricante sobre os demais softwares e hardwares componentes da solução não entrarão nesta contagem, devendo seguir o SLA definido nos requisitos técnicos de cada item da solução.

#### 4.7.4.7. CRITÉRIOS DE SEVERIDADE E TEMPOS DE SOLUÇÃO

SEVERIDADE	EXEMPLOS DE INCIDENTES	TEMPO DE SOLUÇÃO
Alta	Incidente que cause uma falha de processo de backup impedindo a cópia de dados críticos, como registros de processos judiciais e informações sensíveis, resultando na perda irreversível desses dados, na impossibilidade de restauração após um incidente, na interrupção prolongada das atividades, além de possíveis multas e danos à reputação do tribunal por descumprimento de normas de proteção de dados como a LGPD.	06 horas
Média	Incidente de operação que implica em uma falha de um processo de backup parcialmente concluído, resultando na perda temporária de dados não críticos. Ou ainda, pedidos de restauração, backup ou alterações de jobs de backup de informações essenciais.	12 horas
Baixa	Incidente de operação que impacte uma ou mais funcionalidades de baixa criticidade do serviço, porém não compromete a utilização geral do serviço. Bem como, pedidos de restauração, backup ou alterações de jobs de backup de informações essenciais.	24 horas
Requisição	Solicitações diversas ou esclarecimento de dúvidas.	72 horas

#### 4.7.8. INSTRUMENTO DE MEDIÇÃO DE RESULTADOS (IMR) (ITEM 7)

4.7.8.1. A contratação do serviço de gerenciamento técnico e sustentação da solução de proteção de dados será realizada de acordo com a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que estabelece o modelo para a contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação. Conforme o Art. 2º, Parágrafo Único da referida portaria, “o modelo não se configura como de dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho”.

4.7.8.2. O gerenciamento dos níveis de serviço perfaz-se no monitoramento, que evidenciará a qualidade e a tendência dos serviços prestados, e no controle, que alinhará a execução dos serviços aos resultados pretendidos, por meio de um conjunto de procedimentos rotineiros e de regras preestabelecidos neste Termo de Referência.

4.7.8.3. Os NMS devem ser considerados e entendidos pela CONTRATADA como um compromisso de qualidade que está assumindo para a prestação dos serviços. Portanto, no decorrer da execução contratual a CONTRATADA deverá monitorar continuamente seus indicadores, zelando pela qualidade dos seus serviços e pela efetiva entrega de resultados.

4.7.8.4. A CONTRATADA deverá, como parte integrante de suas obrigações contratuais, implementar meios próprios para mensuração dos indicadores de desempenho, realizar o cálculo das eventuais glosas aplicáveis conforme os critérios estabelecidos nos Níveis Mínimos de Serviço (NMS) e aplicá-las previamente na fatura mensal, apresentando junto ao documento fiscal o relatório detalhado com os indicadores apurados, memória de cálculo e valores descontados.

4.7.8.5. A CONTRATANTE realizará verificação independente dos indicadores reportados, sendo que inconsistências entre os dados informados pela CONTRATADA e aqueles apurados pela fiscalização do TJPR serão consideradas como não cumprimento dos Níveis Mínimos de Serviço (NMS), podendo resultar em glosas.

4.7.8.6. Os indicadores serão medidos desde o início da execução contratual, em períodos mensais, e a CONTRATADA será informada dos resultados, para que providencie as eventuais adequações que se fizerem necessárias.

4.7.8.7. Durante os primeiros 90 dias após a emissão do Termo de Recebimento Definitivo, entende-se que a CONTRATADA deverá se ajustar às premissas, objetivos e exigências da CONTRATANTE, e, portanto, não serão aplicadas glosas nesse período.

4.7.8.8. Eventualmente poderão existir impedimentos técnicos para o atendimento dos prazos previamente estabelecidos para uma demanda ou indicador. Nesses casos, a CONTRATADA deverá notificar formalmente o CONTRATANTE – ficando a critério exclusivo deste último avaliar os impedimentos, assim como acatar ou rejeitar as justificativas apresentadas.

4.7.8.9. Em todo o caso, às ocorrências de descumprimento dos Níveis Mínimos de Serviço (NMS) a CONTRATADA poderá interpor justificativas técnicas embasadas em fatos e circunstâncias objetivas, cabendo ao CONTRATANTE avaliar e decidir sobre as alegações. Quando acatadas as justificativas o CONTRATANTE poderá desconsiderar a(s) ocorrência(s) de descumprimento em questão, ajustar os prazos avaliados ou, ainda, suspender a aplicação de eventuais ajustes, quando for o caso.

4.7.8.10. A interposição de justificativas técnicas deverá ser realizada de forma específica para cada caso concreto, não serão admitidas e nem serão objeto de consideração as justificativas que façam referência às ocorrências, fatos ou circunstâncias de modo genérico.

4.7.8.11. A superação de uma ou mais metas de Níveis Mínimos de Serviço (NMS) não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período e/ou o não atendimento da mesma meta em outro período.

4.7.8.12. A ocorrência de reiteradas falhas no cumprimento de prazos, produtividade e de qualidade dos serviços, caracterizará desídia da CONTRATADA e ensejará a aplicação de penalidades previstas, que terão natureza de sanção e serão objeto de processo administrativo próprio – garantido o contraditório e a ampla defesa.

#### 4.7.8.13. ÍNDICE DE CHAMADOS RESOLVIDOS DENTRO DO PRAZO

ATRIBUTO	DESCRIÇÃO
Finalidade	Apurar a eficácia na resolução de chamados (Soluções) estabelecido conforme os NÍVEIS MÍNIMOS DE SERVIÇO (NMS)
Meta a cumprir	Superior ou igual a 95% de chamados (Soluções) resolvidos dentro do prazo
Instrumento de medição	Medição através de registros existentes na Solução de Informação e Gestão de Atendimento – SIGA, ou ferramenta que venha a substituí-lo, durante determinado período, ou ser exportado para uma ferramenta de Business Intelligence (BI)
Forma de acompanhamento	O acompanhamento será realizado por meio de ferramentas (SIGA/BI) ou por meio de procedimentos de amostragens aleatórias
Periodicidade	Mensal
Mecanismo de cálculo	$(\text{Total de chamados resolvidos dentro do prazo} / \text{Total de chamados recebidos (Soluções)}) \times 100$
Início da vigência	O indicador será medido a partir do 1º dia de cada mês
Ajuste no pagamento	1) inferior a 95% e superior ou igual a 85% sofrerá glosa de 3% sobre o valor da fatura corrente referente ao item 7. 2) inferior a 85% sofrerá glosa de 5% sobre o valor da fatura corrente referente ao item 7; 3) Se inferior a 70% aplica-se, além da glosa prevista acima (2), a TABELA DE CONDUTAS 1, ID 1

#### 4.7.8.14. PRAZOS DE INÍCIO E FINALIZAÇÃO DE ATENDIMENTO

TIPO	DESCRIÇÃO	CRITICIDADE	PRAZO
Prazo de Atendimento	Prazo entre a recepção do chamado e o início da execução.	Qualquer	15 Minutos
Prazo de Solução	Tempo até a finalização do chamado	Alto	1 horas
Prazo de Solução	Tempo até a finalização do chamado	Médio	3 horas
Prazo de Solução	Tempo até a finalização do chamado	Baixo	6 horas

#### 4.8. DIREITOS DE PROPRIEDADE INTELECTUAL

4.8.1. A CONTRATADA, nos termos do art. 93 da Lei 14.133/2021, cederá ao



CONTRATANTE, em caráter definitivo, todos os direitos patrimoniais sobre os resultados produzidos no âmbito dos serviços contratados, bem como sobre quaisquer evoluções ou melhorias decorrentes durante a vigência contratual.

4.8.2. Para fins deste contrato, consideram-se “resultados” todos os bens intangíveis gerados – estudos, relatórios, especificações, descrições técnicas, protótipos, dados, planilhas, plantas, desenhos, diagramas, páginas de intranet, códigos-fonte e documentação – em qualquer formato ou mídia.

4.8.3. Componentes de terceiros eventualmente incorporados aos entregáveis permanecerão regidos pelas respectivas licenças. A CONTRATADA garante que tais licenças são compatíveis com o uso irrestrito pelo CONTRATANTE, sem ônus adicional.

4.8.4. É vedada à CONTRATADA a comercialização, cessão ou divulgação dos resultados cedidos, sujeitando-se às penalidades previstas neste instrumento caso descumpra esta obrigação.

4.8.5. Nos itens relativos à aquisição de hardware e de licenças de software comerciais, aplicam-se os direitos autorais e de propriedade intelectual definidos pelos respectivos fabricantes, não havendo geração de novos ativos passíveis de reivindicação pelo CONTRATANTE.

## **4.9. SUBCONTRATAÇÃO E ALTERAÇÃO SUBJETIVA**

4.9.1. Não será permitida a subcontratação do objeto, seja total ou parcial, considerando a necessidade de garantir a responsabilidade técnica integral do fornecedor por toda a solução, bem como assegurar maior controle e eficiência na gestão contratual.

4.9.2. No que diz respeito à alteração subjetiva, é admissível a fusão, cisão ou incorporação da Contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na contratação original; sejam mantidas as demais cláusulas e condições do Termo de Referência; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade à contratação.

## **5. MODELO DE GESTÃO DO CONTRATO**

### **5.1. FISCALIZAÇÃO**

5.1.1. Para a execução do contrato, será implementado método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o Contratante como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues, e a Contratada como responsável pela execução dos serviços e gestão dos recursos humanos e físicos necessários.

5.1.2. A Contratada deve fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus decorrentes de má fiscalização. Esta dar-se-á independentemente daquela que será exercida pelo Contratante.

5.1.3. O Contratante se reserva ao direito de acompanhar e fiscalizar os serviços realizados pela Contratada, verificando a aderência às especificações técnicas definidas, zelando pelo cumprimento dos prazos e monitorando a qualidade dos serviços.

A fiscalização realizada por parte do Contratante não diminui ou atenua a responsabilidade da Contratada pela execução de qualquer serviço.

### **5.2. PRINCIPAIS PAPÉIS**

5.2.1. A Equipe de Gestão da Contratação, designada nas portarias 12658176 e 12659823, é definida na tabela a seguir:

Gestor do Contrato - Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas a coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente do órgão.	Paulo Alfredo Ribas Toledo Técnico em Computação
Gestor Suplente do Contrato - Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas a coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente do órgão.	Simone Sampaio Ribeiro Costa Analista de Sistemas

Fiscal Administrativo - Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.	Maria Aparecida Levis Costa Analista de Sistemas
Fiscal Suplente Administrativo - Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.	Stephanie Wakabayashi Técnica Judiciária
Fiscal Demandante - Servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.	Marco Antonio Gomes Bernardino Analista de Sistemas
Fiscal Técnico - Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.	Diogo Rodrigo Terra Silveira Técnico em Computação Ersan Rafael Holstein Técnico em Computação Maycon Cezar Garcia Penha Técnico em Computação

#### Equipe de Gestão da Contratação

5.2.2. Seus papéis e responsabilidades são definidas no artigo 22, § 3 da Resolução nº 468/2022 do CNJ e descritas no guia de contratações de STIC do Poder Judiciário (páginas 9/12), anexo à referida resolução. Segue abaixo as definições:

5.2.3. Caberá ao **Gestor e Gestor Suplente do Contrato** todas as ações necessárias ao fiel cumprimento das condições estipuladas no contrato e ainda:

- a) analisar a documentação que antecede o pagamento;
- b) analisar os pedidos de reequilíbrio econômico-financeiro do contrato;
- c) analisar eventuais alterações contratuais, após ouvido o fiscal do contrato;
- d) analisar os documentos referentes ao recebimento do objeto contratado;
- e) acompanhar o desenvolvimento da execução através de relatórios e demais documentos relativos ao objeto contratado;
- f) decidir provisoriamente a suspensão da entrega de bens ou a realização de serviços;
- g) efetuar a digitalização e armazenamento dos documentos fiscais e trabalhistas da Contratada no sistema GMS, quando couber, bem como no Portal Nacional de Contratações Públicas (PNCP);
- h) preencher o termo de avaliação de contratos administrativos disponibilizado pelo setor responsável pelo sistema de gestão de materiais, obras e serviços;
- i) inserir os dados referentes aos contratos administrativos no Portal Nacional de Contratações Públicas (PNCP);
- j) iniciar e instruir o procedimento para aplicação das penalidades previstas neste Contrato e na legislação, no caso de constatar irregularidade cometida pela Contratada, encaminhando à comissão competente;
- k) manter controles adequados e efetivos do presente Contrato, do qual constarão todas as ocorrências relacionadas com a execução, inclusive o controle do saldo contratual, com base nas informações e relatórios apresentados pelo fiscal;
- l) tomar as providências relativas à retenção da garantia contratual eventualmente prestada, com a notificação da seguradora da abertura de procedimento

- administrativo em face da empresa Contratada, mantendo-a atualizada sobre o andamento quando solicitado;
- m) verificar a manutenção da necessidade, economicidade e oportunidade da contratação;
- n) propor medidas que melhorem a execução do Contrato;
- o) outras atividades compatíveis com a função.

5.2.4. Caberá aos **Fiscais do Contrato** o acompanhamento da execução do objeto da presente contratação, informando ao gestor as ocorrências que possam prejudicar o bom andamento de sua execução e ainda:

- a) anotar, em registro, próprio todas as ocorrências relacionadas com a execução e determinar o que for necessário à regularização de falhas ou defeitos observados;
- b) esclarecer prontamente as dúvidas administrativas e técnicas e divergências surgidas na execução do objeto contratado;
- c) expedir, através de notificações e/ou relatório de vistoria, as ocorrências e fazer as determinações e comunicações necessárias à perfeita execução dos serviços;
- d) proceder, conforme cronograma físico-financeiro, as medições dos serviços executados e aprovar a planilha de medição emitida pela Contratada ou conforme disposto em contrato;
- e) adotar as medidas preventivas de controle dos contratos, inclusive manifestar-se a respeito da suspensão da entrega de bens, a realização de serviços ou a execução de obras;
- f) conferir e certificar as faturas relativas às aquisições, serviços ou obras;
- g) proceder as avaliações dos serviços executados pela Contratada;
- h) determinar por todos os meios adequados a observância das normas técnicas e legais, especificações e métodos de execução dos serviços exigíveis para a perfeita execução do objeto;
- i) exigir o uso correto dos equipamentos de proteção individual e coletiva de segurança do trabalho;
- j) determinar a retirada de qualquer empregado subordinado direta ou indiretamente à Contratada, inclusive empregados de eventuais subcontratadas, ou as próprias subcontratadas, que, a seu critério, comprometam o bom andamento dos serviços;
- k) receber designação e manter contato com o preposto da Contratada e, se for necessário, promover reuniões periódicas ou especiais para a resolução de problemas na entrega dos bens ou na execução dos serviços ou das obras;
- l) dar parecer técnico nos pedidos de alterações contratuais;
- m) verificar a correta aplicação dos materiais;
- n) requerer das empresas testes, exames e ensaios quando necessários, no sentido de promoção de controle de qualidade da execução das obras e serviços ou dos bens a serem adquiridos;
- o) realizar, na forma do art. 140 da Lei Federal nº 14.133/2021, o recebimento do objeto contratado, quando for o caso;
- p) propor à autoridade competente a abertura de procedimento administrativo para apuração de responsabilidade;
- q) atestar, em documento hábil, o fornecimento, a entrega, a prestação de serviço ou a execução da obra, após conferência prévia do objeto contratado encaminhar os documentos pertinentes ao gestor;
- r) confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no Contrato;
- s) verificar se o prazo de entrega, especificações e quantidades encontram-se de acordo com o estabelecido no instrumento contratual;
- t) informar, em prazo hábil no caso de haver necessidade de acréscimos ou supressões no objeto do Contrato ao gestor do Contrato;
- u) outras atividades compatíveis com a função.

**5.2.5. Fiscal Técnico** – é o servidor representante da área de TI formalmente designado para acompanhar a execução do objeto que tenha sido contratado, com o objetivo de avaliar se a quantidade e qualidade dos serviços estão de acordo com o definido em contrato. Para isso, deverá ter conhecimento técnico do objeto e de todos os termos contratuais que irá fiscalizar, principalmente das condições constantes do edital e de seus anexos, com vistas a acompanhar as obrigações in loco tanto da administração contratante quanto da contratada.

**5.2.5.1. Atribuições do Fiscal Técnico:**

- a) anotar, em registro, próprio todas as ocorrências relacionadas com a execução e determinar o que for necessário à regularização de falhas ou defeitos observados;
- b) esclarecer prontamente as dúvidas administrativas e técnicas e divergências surgidas na execução do objeto contratado;
- c) expedir, através de notificações e/ou relatório de vistoria, as ocorrências e fazer as determinações e comunicações necessárias à perfeita execução dos serviços;
- d) adotar as medidas preventivas de controle dos contratos, inclusive manifestar-se a respeito da suspensão da realização de serviços;
- e) conferir e certificar as faturas relativas aos serviços;
- f) proceder as avaliações dos serviços executados pela CONTRATADA;
- g) determinar por todos os meios adequados a observância das normas técnicas e legais, especificações e métodos de execução dos serviços exigíveis para a perfeita execução do objeto;
- h) determinar a retirada de qualquer empregado subordinado direta ou indiretamente à Contratada, inclusive empregados de eventuais subcontratadas, ou as próprias subcontratadas, que, a seu critério, comprometam o bom andamento dos serviços;
- i) receber designação e manter contato com o preposto da CONTRATADA e, se for necessário, promover reuniões periódicas ou especiais para a resolução de problemas na execução dos serviços;
- j) dar parecer técnico nos pedidos de alterações contratuais;
- k) verificar a correta aplicação dos materiais;
- l) requerer das empresas testes, exames e ensaios quando necessários, no sentido de promoção de controle de qualidade dos serviços a serem executados;
- m) realizar, na forma do art. 140 da Lei Federal nº 14.133/2021, o recebimento do objeto contratado, quando for o caso;
- n) propor à autoridade competente a abertura de procedimento administrativo para apuração de responsabilidade;
- o) atestar, em documento hábil, a prestação de serviço após conferência prévia do objeto contratado encaminhar os documentos pertinentes ao gestor;
- p) confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no Contrato;
- q) verificar se o prazo de entrega, especificações e quantidades encontram-se de acordo com o estabelecido no instrumento contratual;
- r) informar, em prazo hábil no caso de haver necessidade de acréscimos ou supressões no objeto do Contrato ao gestor do Contrato;
- s) outras atividades compatíveis com a função.

**5.2.6. Fiscal Administrativo** – é o servidor designado para acompanhar os aspectos administrativos do ajuste.

**5.2.6.1. São atribuições desse fiscal:**

- a) participar das reuniões iniciais de trabalho e de conclusão da execução contratual;
- b) organizar arquivos específicos para acompanhamento da execução do contrato e para registro de observações e recomendações relativas a contratos de mesma natureza feitas pela Consultoria Jurídica, pelo Departamento de Auditoria Interna e

- pela Coordenadoria de Governança, Riscos e Conformidade, bem como as ocorrências que impactem a execução do contrato ou o futuro TR;
- c) verificar e manter organizada, no início e durante a vigência, cópia do contrato e suas alterações (apostilamento e termo aditivo), bem como da documentação e qualificação exigida dos profissionais alocados no contrato, devendo informar ao gestor as pendências constatadas;
  - d) cadastrar e atualizar as credenciais dos colaboradores da CONTRATADA, bem como solicitar, às áreas de TI, a baixa dessas credenciais dos colaboradores desligados do contrato;
  - e) estabelecer rotina para acompanhar a frequência, a jornada de trabalho, os serviços e funções exercidos pelos colaboradores da CONTRATADA, conforme regras estabelecidas no contrato;
  - f) conferir se os documentos apresentados pela contratada correspondem aos prestadores de serviço que estão alocados para cumprimento do objeto pactuado;
  - g) conferir a documentação exigida em contrato para a realização do pagamento, especialmente, a que se refere as certidões negativas da empresa;
  - h) analisar em conjunto com o fiscal técnico, os documentos apresentados para pagamento juntamente com a Nota Fiscal, conferi-los com as condições estabelecidas no contrato e submeter ao gestor para ateste ou para notificação da contratada de impropriedade constatada;
  - i) realizar, em conjunto com o gestor e fiscal técnico, pesquisa de mercado visando à comprovação da vantagem econômica da contratação, na periodicidade prevista no contrato. A pesquisa de mercado deverá observar as normas vigentes;
  - j) instruir e submeter ao gestor do contrato o pedido de prorrogação contratual, mediante a juntada da documentação que habilitou a contratada devidamente atualizada, bem como da pesquisa de mercado e avaliação dos resultados obtidos que comprovem a necessidade e a vantagem econômica da contratação;
  - k) informar ao gestor do contrato a execução dos saldos empenhados com o auxílio da Secretaria de Finanças.

**5.2.7. Fiscal Demandante** – servidor(es) da área demandante dos serviços. A ele caberá a verificação dos indicativos de atendimentos, bem como os índices de satisfação do usuário, além de:

- a) anotar as ocorrências relacionadas com a execução do contrato, informando ao gestor aquelas que dependam de providências, com vistas à regularização das faltas ou defeitos observados;
- b) avaliar constantemente a qualidade da execução contratual, propondo, sempre que cabível, medidas que visem reduzir gastos e racionalizar os serviços;
- c) solicitar, quando for o caso, a substituição dos serviços por inadequação ou vícios que apresentem;
- d) atestar, mensalmente, o fiel cumprimento das obrigações contratuais assumidas, no que tange à satisfação do usuário, ao material empregado, rotina e qualidade na execução contratual;
- e) identificar as cláusulas do contrato que necessitam de acompanhamento específico;
- f) atuar em tempo hábil na solução dos problemas que porventura venham a ocorrer ao longo da execução contratual.

**5.2.8. Preposto** – representante da CONTRATADA, formalmente designado e responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual. Cabe ao preposto participar da iniciação contratual, encaminhar os pedidos, acompanhar e monitorar sua execução garantindo que sejam atendidos no prazo e na qualidade exigida, atuar na transição contratual e encerramento do contrato.

5.2.8.1. A CONTRATADA deverá manter preposto, aceito pelo CONTRATANTE, durante o período de vigência do contrato, para representá-la administrativamente sempre que for necessário, o qual deverá ser indicado mediante declaração onde deverá constar o nome completo, nº do CPF, do documento de identidade, telefone e e-mail para contato, além dos dados relacionados à sua qualificação profissional.

5.2.9. Os membros da equipe de fiscalização de contratos promoverão o registro das ocorrências verificadas, durante a execução do contrato adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ do art. 117 da Lei nº 14.133/2021.

5.2.10. A fiscalização não excluirá nem reduzirá a responsabilidade do contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e não implicará em corresponsabilidade da Administração ou de seus agentes e prepostos.

5.2.11. Os servidores da equipe de fiscalização de contratos poderão sustar, recusar, mandar fazer e refazer quaisquer serviços que estejam em desacordo com a solicitação e/ou especificação técnica constantes deste TR, determinando o prazo para a correção de possíveis falhas ou substituições de produtos em desconformidade com o solicitado.

5.2.12. As decisões e providências sugeridas formalmente pela CONTRATADA ou julgadas imprescindíveis, que ultrapassem as competências dos membros da equipe de gestão de contratos, deverão ser encaminhadas formalmente por servidor da equipe de fiscalização de contratos à autoridade superior, para a adoção das medidas cabíveis.

5.2.13. Ao TJPR fica assegurado o direito de exigir o cumprimento de todos os itens constantes deste TR, da Proposta da CONTRATADA e das cláusulas contratuais acordados e demais normativos técnicos e administrativos deste Poder Judiciário.

### **5.3. GARANTIA CONTRATUAL**

5.3.1. Não será exigida garantia de execução, uma vez que a contratação se refere à subscrição de licença acompanhada de suporte do fabricante, o que reduz significativamente o risco de inexecução contratual.

5.3.2. Ademais, a contratação contempla a prestação de serviços com pagamentos mensais, efetuados exclusivamente após o efetivo cumprimento e o devido aceite das obrigações contratuais, o que mitiga o risco de desembolso financeiro em caso de eventual inadimplemento.

5.3.3. Nessa hipótese, eventual penalidade de multa poderá ser compensada por meio de desconto em pagamentos futuros, ao longo da vigência contratual.

5.3.4. Considerando essa estrutura da contratação já engloba mecanismos suficientes e eficazes para recomposição de eventuais prejuízos, sem a necessidade de onerar a contratação com exigência de garantia financeira.

### **5.4. OBRIGAÇÕES DA CONTRATADA**

#### **5.4.1. Segurança Institucional**

5.4.1.1. A Contratada será expressamente responsabilizada quanto à manutenção de sigilo sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos e serviços, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos, sob pena de aplicação de sanção na forma prevista no item 5.8. CADERNO DE PENALIDADES. A empresa Contratada deverá manter sigilo sobre todo e qualquer assunto de interesse do TJPR ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

5.4.1.2. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas, padrões e regulamentos e procedimentos estabelecidos na Política de Segurança da Informação do Contratante;

5.4.1.3. Quando nas dependências do TJPR, os técnicos da Contratada ficarão sujeitos a todas as normas internas de segurança do TJPR, inclusive aqueles referentes à identificação, trajés,

trânsito e permanência em suas dependências. A empresa Contratada deverá respeitar as normas e procedimentos de controle e acesso às dependências do TJPR.

5.4.1.4. Quando no ambiente do TJPR, manter os seus funcionários sujeitos às suas normas disciplinares, porém sem qualquer vínculo empregatício com o órgão.

5.4.1.5. Demais questões relativas à Segurança da Informação não previstas no Edital obedecerão à Política de Segurança da Informação do TJPR e a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). A empresa Contratada deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas, padrões e regulamentos estabelecidos na Política de Segurança da Informação do TJPR.

5.4.1.6. A fim de resguardar a segurança institucional, a Contratada não poderá veicular publicidade acerca dos serviços contratados, sem autorização, por escrito, do Contratante.

5.4.1.7. A empresa Contratada não poderá divulgar, mesmo em caráter estatístico, quaisquer informações originadas no TJPR sem prévia autorização formal.

5.4.1.8. A solução Contratada deverá ser de uso exclusivo do Contratante, não havendo possibilidade de compartilhamento de acesso lógico por outras redes, devendo haver confidencialidade no tráfego de rede gerado pelo Contratante.

5.4.1.9. A empresa Contratada deverá substituir imediatamente qualquer um de seus profissionais caso sejam considerados inconvenientes à boa ordem e às normas disciplinares do TJPR.

5.4.1.10. Manter, ainda, os seus funcionários e prepostos identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do TJPR.

5.4.1.11. Utilizar, exclusivamente, pessoal habilitado à prestação dos serviços para os quais se obrigou.

5.4.1.12. A Contratada deverá atender as disposições da Lei Geral de Proteção de Dados (nº 13.709/2018), com o compromisso de se abster de qualquer atividade que constitua uma violação das disposições da Lei; admitir o tratamento dos dados pessoais da Contratada nos termos da Lei; vedar o tratamento de dados pessoais e sensíveis a que tiver acesso, com objetivo de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei Federal nº 13.709/18; dar ciência prévia ao Contratante para fazer uso dos dados privados, sempre zelando pelos princípios da minimização da coleta, necessidade de exposição específica da finalidade, sem prejuízo da mera correção dos dados, em especial quanto aos registros de acesso (logs).

5.4.1.13. Além disso, deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pelo Contratante, as configurações de hardware e de softwares decorrentes e todas as informações do projeto.

## **5.4.2. Deveres e Responsabilidades da Contratada**

5.4.2.1. Envidar todo o empenho necessário ao fiel e adequado cumprimento dos encargos que lhe são confiados.

5.4.2.2. Apresentar, na data da assinatura do contrato, declaração assinada pelo representante legal da empresa indicando preposto para representá-la durante a execução e atuar como interlocutor principal junto ao Contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

5.4.2.3. Fornecer o(s) produtos(s) e/ou serviços conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e no Termo de Referência e no Contrato.

5.4.2.4. Responder por todas as despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias, passagens, diárias, hospedagem, alimentação, hora extra e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que eles não têm nenhum vínculo empregatício com o Contratante.

5.4.2.5. Obedecer às normas técnicas, de saúde, de higiene e de segurança do trabalho, de acordo com as normas do MTE.

5.4.2.6. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços e fiscalizar o uso, em especial pelo que consta da Norma Regulamentadora nº 6 do MTE.

5.4.2.7. Manter, durante toda a execução do contrato, todas as condições de habilitação exigidas para a contratação.

5.4.2.8. Disponibilizar central de atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas no Edital.

5.4.2.9. Comunicar formal e imediatamente ao Gestor ou Fiscal Técnico do TJPR sobre mudanças nos dados para contato com a central de atendimento.

5.4.2.10. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do TJPR, referentes a qualquer problema detectado ou ao andamento de atividades da garantia e/ou dos serviços contratados.

5.4.2.11. Respeitar as normas e procedimentos de controle e acesso às dependências do TJPR;

5.4.2.12. Manter, ainda, os seus funcionários e prepostos identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do TJPR;

5.4.2.13. 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 TJPR;

5.4.2.14. Responder pelos danos causados diretamente à administração do TJPR ou a terceiros, decorrentes de sua culpa ou dolo, durante o fornecimento e a execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento pelo TJPR, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

5.4.2.15. Responder, ainda, por quaisquer danos causados diretamente aos equipamentos ou a outros bens de propriedade do TJPR, quando esses tenham sido ocasionados por seus funcionários durante o fornecimento e a prestação dos serviços, incluindo funcionários terceirizados pela Contratada, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

5.4.2.16. Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

5.4.2.17. Arcar com despesa decorrente de qualquer infração seja qual for, desde que praticada por seus funcionários no recinto do TJPR ou através de acesso remoto.

5.4.2.18. Comunicar ao TJPR qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.

5.4.2.19. Comunicar ao Contratante, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização.

5.4.2.20. Manter em compatibilidade com as obrigações a serem assumidas, durante toda a execução do contrato, todas as condições de habilitação e de qualificação na licitação.

5.4.2.21. Cumprir com os prazos estipulados no Termo de Referência / Edital.

5.4.2.22. Autorizar e assegurar o TJPR o direito de fiscalizar, sustar e/ou recusar os produtos e/ou serviços que não estejam de acordo com as especificações estabelecidas no termo de referência, no edital, no contrato e em todos os seus anexos.

5.4.2.23. Manter sigilo sobre todo e qualquer assunto de interesse do TJPR ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

5.4.2.24. Todas as taxas e impostos que incidam ou venham a incidir sobre este



contrato ou sobre os serviços a ele vinculados correrão por conta da Contratada.

5.4.2.25. Responsabilizar-se integralmente pela execução dos serviços e pelo fornecimento dos produtos, peças, serviços e materiais necessários e indispensáveis à boa execução dos serviços de garantia técnica, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas.

5.4.2.26. Manter em compatibilidade com as obrigações a serem assumidas, durante toda a execução e as condições de habilitação e de qualificação na licitação.

5.4.2.27. Assumir as despesas decorrentes do transporte a ser executado em função do objeto do Contrato.

5.4.2.28. A Contratada deverá aceitar, nas mesmas condições contratuais, os acréscimos que se fizerem no objeto contratual, de acordo com a Lei, em até 25% do valor contratado, mantidas as condições estipuladas no presente Termo de Referência, sem que caiba à Contratada qualquer reclamação.

5.4.2.29. Cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz e, sempre que solicitado pelo Contratante, a Contratada deverá comprovar o cumprimento da reserva de cargos, com a indicação dos empregados que preencherem as referidas vagas.

5.4.2.30. Declarar ciência do conteúdo do Decreto Judiciário nº 62/2026, que institui a Política de Relacionamento do Tribunal de Justiça do Estado do Paraná, bem como do Código de Ética e Conduta do Poder Judiciário do Estado do Paraná, comprometendo-se a observá-los integralmente durante a execução contratual.

a) Decreto Judiciário nº 62/2026 disponível em: <https://www.tjpr.jus.br/legislacao-atos-normativos/-/atos/documento/4760362>

b) Código de Ética e Conduta do Poder Judiciário do Estado do Paraná disponível em: <https://www.tjpr.jus.br/web/comissao-de-etica-e-de-conduta/codigo-de-etica-e-conduta>

## **5.5. OBRIGAÇÕES DO CONTRATANTE**

5.5.1. Proporcionar à Contratada todas as facilidades necessárias ao cumprimento do contrato, inclusive acesso remoto ao software objeto do contrato, quando devidamente justificado e sob as condições de segurança e sigilo pactuadas indispensáveis à boa execução das obrigações contratuais, inclusive permitindo o acesso de empregados, prepostos ou representantes da Contratada às dependências do Tribunal.

5.5.2. Designar responsáveis para o acompanhamento e fiscalização da execução do objeto contratual.

5.5.3. Estabelecer normas e procedimentos de acesso às suas instalações para a execução de serviços.

5.5.4. Informar à Contratada de atos que possam interferir direta ou indiretamente nos serviços prestados.

5.5.5. Comunicar formalmente qualquer anormalidade ocorrida na execução do objeto adquirido através deste termo de referência.

5.5.6. Verificar minuciosamente, no prazo fixado, a conformidade dos serviços executados para fins de aceite na ocasião dos faturamentos mensais.

5.5.7. Receber os serviços provisoriamente e definitivamente, mediante termo de recebimento e em conformidade com a legislação.

5.5.8. Atestar as faturas de serviço apresentadas mensalmente pela Contratada, informando imediatamente e por escrito sobre a eventuais glosas a serem aplicadas, justificando seus motivos

5.5.9. Efetuar o pagamento do valor contratado, após o recebimento e aprovação dos serviços executados e após o recebimento definitivo do objeto de acordo com as condições

especificadas e estipuladas nesta licitação.

5.5.10. Permitir o acesso aos técnicos devidamente credenciados pela Contratada às dependências das instalações que contenha o objeto da presente contratação, dentro do horário normal de expediente forense ou além deste, se necessário, em caso de atendimento de suporte técnico, mediante autorização e acompanhamento por servidor designado.

5.5.11. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da Contratada.

5.5.12. Aplicar as sanções conforme previsto no presente termo de referência e/ou no contrato.

5.5.13. Orientar a contratada no que tange à solicitação de emissão de atestados de capacidade técnica quando solicitado, desde que atendidas as obrigações contratuais.

## **5.6. TRANSIÇÃO CONTRATUAL**

5.6.1. Uma nova licitação deverá ser iniciada com antecedência mínima de 18 (dezoito) meses antes do término deste contrato e deverá estar homologada até seis meses antes do seu encerramento, garantindo janela processual suficiente para recursos, impugnações e ajustes, bem como possibilitando sobreposição operacional entre as soluções.

5.6.2. A CONTRATADA apresentará versão preliminar do Plano de Transição em T-18 meses e versão final revisada até T-3 meses do encerramento contratual.

5.6.3. O escopo da transição abrangerá todos os serviços e *workloads* que estejam cobertos pela solução na data de corte, incluindo bancos de dados, máquinas virtuais, Kubernetes/Tanzu, contas Microsoft 365, backups imutáveis e futuras cargas protegidas durante a vigência contratual, assegurando continuidade plena dos serviços jurisdicionais.

5.6.4. A CONTRATADA deverá cooperar com a futura prestadora, disponibilizando exportação de metadados, chaves de criptografia, *runbooks* de operação, relatórios de falhas e demais artefatos necessários, obedecendo a prazos de resposta de até quarenta e oito horas a cada solicitação formal do TJPR.

5.6.5. O plano de transição contratual será executado pelo CONTRATANTE e deverá ocorrer sem custos adicionais.

5.6.6. Após o término do contrato, a CONTRATADA deverá retirar todo e qualquer bem de que seja proprietária e que, eventualmente, esteja alocado nas instalações do CONTRATANTE, assim como providenciar a devolução de recursos que lhe tenham sido eventualmente cedidos pelo CONTRATANTE e, quando for o caso, a desinstalação de recursos de software de sua propriedade mantidos no ambiente do CONTRATANTE.

## **5.7. CADERNO DE PENALIDADES**

### **5.7.1. PENALIZAÇÕES**

5.7.1.1. A Contratada será responsabilizada administrativamente pelas seguintes infrações, conforme previsto na Lei Federal nº 14.133/2021, no Decreto Estadual nº 10.086/2022 e no Decreto Judiciário nº 269/2022-TJ/PR:

- a) dar causa à inexecução parcial do contrato;
- b) dar causa à inexecução parcial do contrato que cause grave dano ao Contratante, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) dar causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- e) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

i) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

5.7.1.1.1. Considera-se inexecução total do contrato a recusa injustificada de cumprimento integral da obrigação contratualmente determinada.

5.7.1.2. A Contratada que incorrer nas infrações administrativas previstas no item 5.7.1.1 sujeitar-se-á às seguintes sanções:

a) **advertência**: exclusivamente pelas infrações administrativas na letra "a" do item 5.7.1.1 e no caso de descumprimento, de pequena relevância, de obrigação legal ou infração à Lei quando não se justificar aplicação de sanção mais grave;

b) **multa** com relação a quaisquer das infrações previstas no item 5.7.1, que será calculada na forma prevista neste Contrato;

c) **impedimento**: pelas infrações administrativas previstas nas letras "b" a "d" do item 5.7.1.1, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos;

d) **inidoneidade**: pelas infrações administrativas previstas nas letras "e" a "i" do item 5.7.1.1, bem como pelas infrações administrativas previstas nas letras "b" a "d" do referido item que justifiquem a imposição de penalidade mais grave de impedimento, e impedirá o responsável de licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

5.7.1.3. Para fins de aplicação da advertência, considera-se pequena relevância o descumprimento de obrigações ou deveres instrumentais ou formais que não impactam objetivamente na execução do contrato, bem como não cause prejuízos ao Contratante.

5.7.1.4. A sanção de advertência, impedimento e inidoneidade poderão ser aplicadas cumulativamente com a multa.

5.7.1.5. As sanções de impedimento e inidoneidade serão aplicadas de modo independente em relação a cada infração diversa cometida.

5.7.1.5.1. Para o cômputo dessas sanções deverão ser observadas as demais regras dos arts. 224 a 225 do Decreto Estadual nº 10.086/2022.

5.7.1.6. A aplicação das sanções previstas nas alíneas do item 5.7.1.2. não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

5.7.1.7. Na aplicação das penalidades serão consideradas as circunstâncias do art. 156, §1º, da Lei Federal nº 14.133/2021, quais sejam:

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para ao Contratante;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

5.7.1.7.1. Deverão ser consideradas como agravantes e atenuantes as circunstâncias previstas nos arts. 211 a 212 do Decreto Estadual nº 10.086/2022.

5.7.1.7.2. O cometimento de mais de uma infração em uma relação contratual sujeitará o infrator à sanção cabível para a mais grave entre elas, ou se iguais, somente uma delas, sopesando-se, em qualquer caso, as demais infrações como circunstância agravante, observando-se, ainda o previsto nos parágrafos do art. 198 do Decreto Estadual nº 10.086/2022.

5.7.1.8. A mora no cumprimento de obrigações contratuais independe de notificação da Contratada (*dies interpellat pro homine*), salvo previsão expressa.

5.7.1.8.1. O cumprimento parcial da parcela em atraso reduzirá proporcionalmente à base de cálculo da penalidade de multa.

5.7.1.9. As sanções de multa moratória não serão cumuladas com a pena de multa prevista para o caso de rescisão contratual, quando a rescisão decorrer da própria mora.

5.7.1.10. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

5.7.1.11. Além do previsto no item 5.7.1.10. poderá configurar a inexecução total da obrigação e a aplicação da penalidade prevista no item 6 da tabela 3, sem prejuízo de eventual indenização pela Contratada derivada de perdas e danos causados ao Contratante (decorrente das infrações cometidas), quando:

- a) a execução do objeto contratado for inferior a 50% (cinquenta por cento) do total;
- b) houver reiterado descumprimento das obrigações assumidas;
- c) o atraso na execução ultrapassar o prazo limite de 30 (trinta) dias corridos e não houver o interesse do Contratante em manter a contratação;
- d) o descumprimento parcial prejudicar a solução como um todo.

5.7.1.11.1. A rescisão do contrato dependerá de análise de oportunidade e conveniência do Contratante.

5.7.1.12. A personalidade jurídica poderá ser desconsiderada administrativamente, conforme previsto no art. 160 da Lei Federal nº 14.133/21, devendo ser observados os procedimentos previstos nos arts. 215 a 223 do Decreto Estadual nº 10.086/2022.

5.7.1.13. Após a regular tramitação do procedimento administrativo para apuração da irregularidade e a aplicação de sanções, incidindo a aplicação da penalidade de multa, a Contratada será notificada para o pagamento.

5.7.1.13.1. Transcorrido o prazo para o pagamento da multa sem o seu adimplemento o Contratante poderá compensar o valor devido com qualquer crédito existente nesta ou em outra contratação.

5.7.1.13.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

5.7.1.13.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

5.7.1.14. Qualquer multa ou encargo imputado à Contratada, não pago no prazo concedido pela Contratante, será inscrito no CADIN Estadual e em Dívida Ativa do Estado e cobrado com base na Lei Federal nº 6.830/1980, sem prejuízo da correção monetária.

5.7.1.15. As disposições desta cláusula de penalidades não excluem a responsabilização da licitante por eventuais atos lesivos previstos na Lei Federal nº 12.846/2013 e demais legislações, bem como a responsabilidade de indenização suplementar em caso de perdas e danos decorrente da conduta.

5.7.1.15.1. Nesses casos, os atos lesivos serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na Lei Federal nº 12.846/2013.

5.7.1.16. Sem prejuízo das demais penalidades, as de multa serão aplicadas conforme detalhamento constante das tabelas abaixo.

5.7.1.16.1. Para a verificação e enquadramento da conduta nas tabelas de penalidades, será considerada em primeiro lugar a conduta específica e somente será aplicada a genérica na falta daquela.

## 5.7.2. TABELA DE CONDUTAS 1:

ID	CONDUTAS	PENALIDADES
----	----------	-------------

ID	CONDUTAS	PENALIDADES
01	Não atendimento das metas estabelecidas nos indicadores dos INSTRUMENTO DE MEDIÇÃO DE RESULTADOS (IMR) (ITEM 7)	Multa de 10% (dez por cento) do valor mensal do contrato relativo ao ITEM 7, pelo indicador descumprido.
02	Atraso na confirmação do recebimento da ordem de serviço conforme Anexo 04 - SLA1	Multa de R\$ 100,00 (cem reais) por dia de atraso.
03	Atraso na elaboração do cronograma e do plano de trabalho conforme Anexo 04 - SLA2	Multa de R\$ 100,00 (cem reais) por dia de atraso.
04	Não atendimento do cronograma ao plano de trabalho conforme Anexo 04 - SLA3	Multa de R\$ 100,00 (cem reais) por dia de atraso. <a href="#">[EH1]</a>
05	Não atendimento no prazo para correções ao plano de trabalho executado conforme Anexo 04 - SLA4	Multa de R\$ 1.000,00 (mil reais) por dia de atraso.
06	Deixar de atender os Níveis Mínimos de Serviço.	Multa de R\$ 1.000,00 (mil reais) por dia de atraso.
07	Deixar de manter, na vigência do contrato, as condições originais de habilitação.	Multa de 2% (dois por cento), por evento, calculada sobre o valor mensal do contrato.
08	Deixar o prestador de serviço da CONTRATADA de respeitar as normas internas de segurança do TJPR, inclusive aqueles referentes à identificação, crachá, trajes e equipamentos adequados, trânsito e permanência, nas dependências do Tribunal de Justiça do Paraná.	Multa no valor fixo de R\$ 200,00 (duzentos reais) por conduta.
09	Deixar de disponibilizar os bens ou serviços, caracterizando a inexecução parcial.	Multa de 0,5% (zero vírgula cinco por cento) a 10% (dez por cento) sobre o valor da parcela inadimplida, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente das infrações cometidas.
10	Descumprimento das exigências de qualificação e capacitação dos profissionais, conforme exigidas para cada tipo de atividade; Ou Não comprovação da qualificação de novos profissionais no prazo estipulado no decorrer da contratação;	Multa de R\$ 500 (quinhentos reais) por profissional não qualificado por dia de descumprimento.

### 5.7.3. TABELA DE CONDUTAS 2:

ID	CONDUTAS	PENALIDADES
01	O atraso injustificado na entrega dos bens ou na prestação do serviço no início da execução do contrato nos prazos estabelecidos neste instrumento contratual.	Aplicar-se-á multa de 0,5% (cinco décimos por cento) do valor da parcela inadimplida por dia de atraso, observado o máximo de 20% (vinte por cento).

ID	CONDUTAS	PENALIDADES
02	Deixar, o prestador de serviço da CONTRATADA, de utilizar crachá de identificação ou não estiver trajando roupas/equipamentos adequados à prestação do serviço, dentro das instalações do CONTRATANTE.	Multa no valor fixo de R\$ 100,00 (cem reais) por conduta.
03	Inobservância do prazo fixado para apresentação da garantia de execução, quando prevista, ainda que seja para reforço/prorrogação de vigência ou Inobservância do prazo fixado para entrega do Formulário de Análise de Perfil das Contratadas do Tribunal de Justiça do Estado do Paraná, quando cabível;	Aplicar-se-á multa de 0,1% (zero vírgula um por cento) do valor do contrato por dia útil de atraso, observado o máximo de 1% (um por cento) do valor global do contrato.
04	Deixar de manter, na vigência do contrato, as condições originais de habilitação, dispostas na legislação vigente.	Multa de 1% (um por cento), por evento, a ser verificado mensalmente, calculada sobre o valor global do contrato.

#### 5.7.4. TABELA DE CONDUTAS 3:

ID	CONDUTAS	PENALIDADE
01	O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos quando não haja previsão de conduta específica ou Quando o preposto ou responsável técnico não se apresentar em reunião pré-agendada.	Primeira vez: Advertência Segunda vez e seguintes: Multa de 0,5% (zero vírgula cinco por cento) a 1% (um por cento) do valor global do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 20% (vinte por cento) do valor da contratação.
02	O não cumprimento de cláusulas contratuais, quando não haja previsão de conduta específica ou O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores ou Quando deixar de substituir prestador de serviço que se portar ou realizar condutas de modo inconveniente ou não atenda às necessidades.	Multa de 0,5% (zero vírgula cinco por cento) a 2% (dois por cento) do valor global do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 20% (vinte por cento) do valor da contratação.
03	A paralisação do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração, quando não haja previsão de conduta específica.	Multa de 0,5% (zero vírgula cinco por cento) a 3% (três por cento) do valor global do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 15% (quinze por cento) do valor global do contrato.

ID	CONDUTAS	PENALIDADE
04	<p>Quando for evidenciado que o prestador de serviço da CONTRATADA realizou atividade de quebra ou ameaça de segurança das informações do Tribunal de Justiça, inseriu código malicioso em sistema, inseriu intencionalmente praga digital na rede do Tribunal de Justiça, obteve acesso não autorizado à informação ou sistema</p> <p>ou</p> <p>Apresentar documento falso ou fazer declaração falsa</p> <p>ou</p> <p>Agir de má-fé na relação contratual</p> <p>ou</p> <p>Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o contrato.</p>	Multa de 10% (dez por cento) a 20% (vinte por cento) do valor global da contratação.
05	<p>Abandonar a execução do contrato</p> <p>ou</p> <p>Incorrer em inexecução total contratual quando não haja previsão de conduta específica</p> <p>ou</p> <p>Tenha sofrido condenação judicial definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos</p> <p>ou</p> <p>Demonstrar não possuir idoneidade para contratar com a Administração, em virtude de atos ilícitos praticados, em especial, infrações à ordem econômica</p> <p>ou</p> <p>Tenha sofrido condenação definitiva por ato de improbidade administrativa, na forma da lei</p> <p>ou</p> <p>A subcontratação total ou parcial do seu objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato</p> <p>ou</p> <p>A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato.</p>	Multa de 2% (dois por cento) a 20% (vinte por cento) sobre o valor global do contrato, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente.
06	<p>Descumprimento ou inexecução total do contrato/obrigações que gere a rescisão contratual.</p>	Multa de 10% (dez por cento) a 20% (vinte por cento) sobre o valor global do contrato, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente das infrações cometidas.

ID	CONDUTAS	PENALIDADE
07	Descumprimento da obrigação de zelo no tratamento dos dados pessoais da pessoa natural vinculada ao CONTRATANTE, ou em caso de tratamento de dados sem o consentimento específico e destacado por termo de compromisso, ou outra irregularidade havida no cumprimento do Contrato, por culpa da CONTRATADA.	Multa de 10% (dez por cento) sobre o valor global do Contrato.
08	Tratar dados pessoais sensíveis com o objetivo de obter vantagem econômica, ou outra irregularidade havida no cumprimento do Contrato, por culpa da CONTRATADA.	Multa de até 20% (vinte por cento) sobre o valor global do Contrato.

## 6. CRITÉRIOS DE RECEBIMENTO E DE PAGAMENTO

### 6.1. RECEBIMENTO

6.1.1. Os produtos e serviços serão aceitos conforme previsto na seção DINÂMICA DA EXECUÇÃO deste TERMO DE REFERÊNCIA.

6.1.2. A entrega dos equipamentos deverá ocorrer nos seguintes endereços Rua Álvaro Ramos, 157 e Praça Nossa Senhora de Salette, S/N, ambos no Bairro: Centro Cívico, Curitiba/PR.

6.1.3. A entrega dos softwares ocorrerá com a disponibilização das licenças em nome do Tribunal de Justiça do Estado do Paraná;

6.1.4. Para cumprimento do contido neste item, fica designada Comissão de Recebimento constituída pelo Chefe da Divisão de Sustentação da Secretaria de Tecnologia da Informação, fiscais técnicos e demandantes;

6.1.5. Os Termos de Recebimentos Definitivos e Termo de Recebimento relativos a horas sob demanda deverão conter a assinatura da Comissão de Recebimento constituída para esse fim. Estes artefatos não excluem a responsabilidade civil da empresa vencedora por vícios qualitativos, quantitativos ou técnicos dos materiais ou por desacordo com as especificações estabelecidas neste Termo de Referência, verificadas posteriormente;

6.1.6. Uma vez constatada a existência de incorreções e defeitos após o recebimento definitivo, a CONTRATADA deverá iniciar procedimento para sanar as irregularidades imediatamente após o recebimento da comunicação efetuada pelo CONTRATANTE, sem prejuízo da aplicação de sanções à empresa.

### 6.2. PAGAMENTO

6.2.1. A CONTRATADA deverá, obrigatoriamente, formular pedido de pagamento e protocolá-lo através de formulário eletrônico disponível no endereço <https://www.tjpr.jus.br/protocolo-admin> (opção “Contratados”). O pedido de pagamento deverá ser apresentado indicando o número do contrato, data de referência, descrição e valor do item, devidamente instruído com a nota fiscal com o CNPJ do CONTRATANTE nº 77.821.841/0001-94 e certidões de regularidade fiscal atualizada;

6.2.2. A CONTRATANTE poderá promover a retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, quando a CONTRATADA não produzir os resultados esperados, deixar de executar ou não executar com a qualidade mínima exigida as atividades contratadas.

6.2.3. Para fins de liberação do pagamento, a Administração efetuará consulta ao Cadastro Informativo Estadual - Cadin Estadual. As pessoas físicas e jurídicas com registro no Cadin Estadual estarão impedidas de receber pagamentos referentes a contratação, na forma do art. 3º da Lei 18.466/2015;

6.2.4. Na hipótese de atraso do pagamento da Nota Fiscal/Fatura devidamente atestada, e desde que para tal não tenha concorrido de alguma forma a CONTRATADA, o valor devido pelo TJPR será atualizado financeiramente, se assim solicitado pela CONTRATADA, obedecendo à legislação vigente;



6.2.5. No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão os mesmos restituídos à CONTRATADA para as correções necessárias, não respondendo o TJPR por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes, haja vista que o prazo para pagamento será interrompido, e terá sua contagem iniciada novamente somente após a apresentação dos documentos corretos;

6.2.6. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação de qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

6.2.7. Os pagamentos à CONTRATADA somente serão efetuados após a verificação do cumprimento das obrigações contratuais e do atendimento às exigências definidas neste Termo de Referência, mediante a apresentação da documentação fiscal correspondente e dos relatórios de execução aprovados pela fiscalização contratual.

#### **6.2.8. CONDIÇÕES PARA LIBERAÇÃO DO PAGAMENTO**

**6.2.8.1. PAGAMENTO DO GRUPO 1 - ITENS 1 a 6:** O pagamento será realizado após a emissão do Termo de Recebimento Definitivo, no prazo de até 30 (trinta) dias corridos, contados a partir do protocolo da solicitação. O pagamento será efetuado mediante requerimento assinado, acompanhado da respectiva nota fiscal/fatura, e após o atesto do fiscal do Contrato.

**6.2.8.2. PAGAMENTO DO GRUPO 1 - ITEM 7:** Os pagamentos mensais serão proporcionais aos serviços entregues e aceitos pelo TJPR, levando-se em consideração o resultado obtido na execução dos serviços, medidos conforme os Níveis Mínimos de Serviço (NMS). Para fins de medição, serão autorizados para faturamento apenas os serviços concluídos e aceitos pelo TJPR. O pagamento será realizado em até 30 (trinta) dias corridos após o protocolo do pedido de pagamento. Após a análise da documentação apresentada pela CONTRATADA e, estando de acordo, o CONTRATANTE autorizará a emissão da Nota Fiscal/Fatura. A CONTRATADA deverá então realizar o protocolo do pedido de pagamento, conforme estabelecido na seção CONDIÇÕES E PRAZOS PARA LIQUIDAÇÃO E PAGAMENTO.

**6.2.8.3. PAGAMENTO DO GRUPO 1 - ITEM 8:** Os pagamentos serão realizados mediante a conclusão dos serviços especializados sob demanda autorizados pelo TJPR. Para o pagamento dos serviços aceitos, será considerado o resultado obtido na sua execução. Serão autorizados para faturamento apenas os serviços concluídos, aceitos pelo TJPR e com a emissão do Termo de Recebimento referente às horas técnicas sob demanda. O pagamento será efetuado em até 30 (trinta) dias corridos após o protocolo do pedido de pagamento. Após a análise da documentação, e estando de acordo, o CONTRATANTE autorizará a emissão da Nota Fiscal/Fatura, e a CONTRATADA deverá protocolar o pedido de pagamento conforme a seção CONDIÇÕES E PRAZOS PARA LIQUIDAÇÃO E PAGAMENTO.

#### **6.3. REAJUSTE**

6.3.1. Serão passíveis de reajustes apenas os itens 7 e 8. Estes preços serão fixos e irreajustáveis pelo prazo de um ano, contado da data do orçamento estimado.

6.3.2. Poderá ser negociado um reajuste dos preços contratados mediante solicitação fundamentada da CONTRATADA, desde que observados os valores praticados no mercado e com base no Índice de Custo de Tecnologia da Informação (ICTI) ou, na impossibilidade de utilização deste, no Índice de Preços ao Consumidor Amplo (IPCA). Esse reajuste será aplicável apenas às obrigações iniciadas e concluídas após a ocorrência da anualidade.

### **7. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

#### **7.1. MODALIDADE, TIPO DE LICITAÇÃO**

7.1.1. Verifica-se que os produtos e serviços aqui pretendidos são oferecidos por diversas empresas do mercado de TIC e apresentam características padronizadas e usuais. Assim, pode-se concluir, a princípio, que são de natureza “comum” e, portanto, poderá ser utilizada a modalidade “Pregão”, o modo de disputa será o ABERTO, o critério de julgamento será pelo MENOR VALOR e será considerado o PREÇO TOTAL/GLOBAL, sendo que o intervalo entre os lances para cada um dos itens não poderá ser inferior aos indicados na tabela abaixo, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

### 7.1.2. INTERVALO MÍNIMO DE LANCES

ITEM	DESCRIÇÃO	INTERVALO MÍNIMO
1	Software de Proteção de Dados	R\$ 10.000,00
2	Servidor de Armazenamento de alta performance	R\$ 100,00
3	Appliances de Armazenamento de alta densidade	R\$ 1.000,00
4	Serviço - Instalação, Configuração e Migração dos Jobs	R\$ 10,00
5	Serviço – Capacitação no Software de Proteção de Dados	R\$ 10,00
6	Serviço – Capacitação no Appliances de Armazenamento de alta densidade	R\$ 10,00
7	Serviço de Gerenciamento Técnico e Sustentação da Solução de Proteção de Dados	R\$ 1000,00
8	Serviço - Horas Técnicas Especializadas sob demanda	R\$ 1,00

7.1.2.1. Não será permitida a participação de empresas em consórcio, tendo em vista que existem no mercado fornecedores com capacidade de entregar isoladamente a solução completa, não se justificando a complexidade adicional de gestão que os consórcios representariam.

### 7.2. PROPOSTA DE PREÇOS

7.2.1. A proposta de preços deverá ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar:

a) Identificação social, número do CNPJ, assinatura do representante legal da proponente, referência a esta licitação, número de telefone, endereço, dados bancários, número de fax e indicação de endereço eletrônico (e-mail);

b) O prazo de validade da proposta é de 90 (noventa) dias, a contar da data de abertura da sessão pública estabelecida no preâmbulo deste Edital;

c) Indicação única de preço (R\$), com exibição dos valores unitário, em algarismos, e total/global, em algarismos e por extenso, conforme o lance final respectivo;

d) Declaração dirigida ao TJPR afirmando que disponibilizará, a partir da assinatura do contrato, Central de Atendimento para abertura de chamado de assistência técnica para o produto cotado e em conformidade com as exigências quanto aos requisitos de suporte e garantia técnica especificados neste termo de referência.

e) Declaração de que a garantia, suporte técnico “on-site” na cidade de Curitiba e o SLA, será CONTRATADA com o fabricante, pelo período de, no mínimo, 60 (sessenta) meses para toda solução, contados da emissão do respectivo Termo de Recebimento Definitivo, atendidas todas as condições estabelecidas no edital – Termo de Referência; (não se aplica para o item 8).

f) Declaração de que a empresa licitante é a fabricante do equipamento ou revendedora autorizada dos produtos pelo fabricante;

g) A indicação do fabricante (marca) e do modelo/série/SKU do produto ou serviço ofertado. O modelo indicado não pode ser genérico e deve possibilitar a conferência das características do produto através dos canais de comercialização do fabricante no Brasil (manuais ou outro documento oficial do fabricante);

h) Documentação técnica, obrigatoriamente em formato digital do tipo PDF, comprovando que os produtos ofertados atendem as especificações técnicas mínimas obrigatórias conforme REQUISITOS TÉCNICOS, devendo ainda, informar em uma planilha cada item relacionado nas especificações técnicas, indicando em que documento, página e parágrafo se encontra a comprovação. Caso não seja possível a comprovação com a indicação fornecida a PROPONENTE será desclassificada;

h.1) Havendo divergência entre as características técnicas descritas na proposta da empresa e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pelo TJPR;

h.2) A simples apresentação de proposta com a "repetição" das especificações técnicas exigidas neste Termo de Referência não garante o atendimento integral do objeto;

h.3) Não serão consideradas afirmações sem a devida comprovação técnica ou documental;

i) Declaração de que não se beneficiará, junto ao fabricante, de vantagens decorrentes do registro de oportunidade para parceiros comerciais ou prática semelhantes em detrimento dos demais concorrentes

j) Declaração da licitante de que disponibilizará, na fase de planejamento, técnico certificado pelo fabricante dos equipamentos fornecidos em suas tecnologias e funções, bem como disponibilizará, na fase de execução do projeto, técnico de forma presencial para instalação, configuração e ativação dos equipamentos fornecidos nas dependências do TJPR.

k) Declaração do licitante ou fabricante que os equipamentos referentes aos itens 2 e 3 não se encontram na situação de "solicitação de venda encerrada" ("end of sale") ou "solicitação de pedido suspensa" ("end of order") ou "fim do suporte" ("end of support") ou "fim da vida útil" ("end of life") pelo fabricante;

7.2.2. A proposta deve levar em conta todos os custos operacionais para o período de vigência da contratação, inclusive quanto à reoneração gradual prevista para os anos de 2025 e 2026. Assim, a reoneração gradual, por ser previamente de conhecimento da Contratada, não será fato ensejador de reequilíbrio econômico-financeiro.

### 7.2.3. TABELA MODELO PARA PROPOSTAS

Item	Descrição	Valor Unitário	Valor Total
1	Software de Proteção de Dados		
2	Servidor de Armazenamento de alta performance		
3	Appliances de Armazenamento de alta densidade		
4	Serviço - Instalação, Configuração e Migração dos Jobs		
5	Serviço – Capacitação no Software de Proteção de Dados		
6	Serviço – Capacitação no Appliances de Armazenamento de alta densidade		
7	Serviço de Gerenciamento Técnico e Sustentação da Solução de Proteção de Dados *		
8	Serviço - Horas Técnicas Especializadas sob demanda		
* O montante proposto para o item 7 deve seguir as diretrizes da Portaria SGD/MGI nº 1.070, especialmente os valores previstos no Anexo II – Mapa de Pesquisa Salarial de Referência para Serviços de Operação de Infraestrutura e Atendimento ao Usuário, aplicáveis ao CBO 2124-20 (Analista de Suporte Computacional Sênior), função correlata à de Analista de Backup. Ressalta-se que o salário do colaborador não poderá ser inferior ao estabelecido nessa portaria para a função mencionada.* A CONTRATADA deverá ainda entregar a Planilha de Composição de Custos e Formação de Preços contida no ANEXO 06, referente ao item 7			

### 7.3. QUALIFICAÇÃO TÉCNICA

7.3.1. A empresa PROPONENTE deverá apresentar comprovação de capacidade técnica operacional, por meio de Atestado de Capacidade, expedido por pessoa jurídica de direito público ou privado, com a identificação da empresa ou órgão público, atestando que a licitante forneceu os equipamentos, presta ou está prestando os serviços.

### 7.3.2. REQUISITOS PARA EMISSÃO DO ATESTADO DE CAPACIDADE TÉCNICA

ITEM	DESCRIÇÃO	UNIDADE	QUANTITATIVO MÍNIMO
1	Software de Proteção de Dados	Terabytes Protegidos	250
3	Appliances de Armazenamento de alta densidade - Appliances ou área de armazenamento dedicada utilizada para repositório backup em armazenamento em bloco ou objeto.	Terabytes	250
4	Serviço - Instalação, Configuração e Migração dos Jobs	Jobs migrados	50

ITEM	DESCRIÇÃO	UNIDADE	QUANTITATIVO MÍNIMO
7	Serviço - Gerenciamento Técnico e Sustentação da solução de proteção de dados.	Meses de Serviços Prestados	24

7.3.2.1. Para fins de comprovação do ITEM 3, serão aceitos atestados de capacidade técnica que comprovem o fornecimento de soluções de armazenamento utilizadas em ambientes de backup, incluindo, mas não se limitando a: *appliances* dedicados, *storages* tradicionais ou *object storages*, desde que apresentem complexidade tecnológica e operacional equivalente ou superior ao objeto ora licitado.

7.3.2.2. Em relação ao item 4 “Serviço - Instalação, Configuração e Migração dos Jobs” – envolve atividades críticas para a implantação da solução, segurança da informação e continuidade dos serviços institucionais. Essas atividades representam parcelas de maior relevância do contrato, pois são diretamente responsáveis pela integridade e disponibilidade dos dados corporativos. O número mínimo de *Jobs* a migrar totalizam 150, conforme especificado no item 2.6 DIMENSIONAMENTO DA SOLUÇÃO.

7.3.2.3. Em conformidade com o § 1º do art. 67 da Lei nº 14.133/2021, a exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual igual ou superior a 4% do valor total estimado da contratação. A instalação e configuração da solução de backup e restore enquadram-se nessa definição, dado seu impacto estratégico e elevado risco operacional.

7.3.2.4. Além disso, conforme ensina Joel de Menezes Niebuhr, “ *O legislador, aqui, preferiu a conjunção ou. Então, na Lei nº 14.133/2021, as exigências de qualificação técnica não precisam ser, ao mesmo tempo, relevantes sob o ponto de vista técnico e econômico. Porém, ser um ou outro, ou tecnicamente relevantes ou economicamente relevantes.*” Assim, a exigência fundamenta-se na relevância técnica da parcela, independentemente do valor econômico, reforçando a legalidade da medida.

7.3.2.5. A solicitação de atestados de capacidade técnica para o item 4 da solução é justificada pela necessidade de comprovar experiência diversificada em ambientes complexos, garantindo que o licitante tenha atuado em diferentes cenários e seja capaz de executar o serviço com segurança e eficiência. Essa exigência é proporcional, razoável e fundamentada na legislação e na doutrina, não restringindo a competitividade, pois permite o somatório de atestados para atingir a capacidade requerida.

7.3.2.6. O(s) atestado(s) deverá(ão) conter, no mínimo, as seguintes informações:

- Identificação da pessoa jurídica emitente bem como o nome e o cargo do signatário;
- Discriminação do serviço prestado;
- Volume ou quantidade de serviços realizados;
- Prazo contratual com data de início dos serviços;
- Caracterização do bom desempenho do licitante;
- Outros dados característicos se houver; (mais específico);
- O documento deverá ser apresentado em papel timbrado do emitente;
- Será admitido o somatório de atestados.

7.3.2.7. A licitante poderá disponibilizar todas as informações que entender necessárias à comprovação da legitimidade dos atestados.

7.3.2.8. Não serão admitidos atestados emitidos por empresas pertencentes ao mesmo grupo econômico da proponente. Consideram-se pertencentes ao mesmo grupo econômico as entidades que embora tendo, cada uma delas, personalidades jurídicas próprias, mantiverem, entre si, direta ou indiretamente, relação de controle (art. 1.098 do Código Civil), ou estiverem sob o controle, direção ou administração, direta ou indireta, de outra pessoa física ou jurídica em comum;

7.3.2.9. O(s) atestado(s) de capacidade poderá(ão) ser objeto(s) de diligência, a critério deste Tribunal de Justiça, para verificação de autenticidade de seu(s) conteúdo(s). Poderá ser solicitado da licitante a apresentação de documentos como, por exemplo, contratos, notas de empenho

ou notas fiscais etc.;

7.3.2.10. Encontrada divergência entre o especificado nos atestados e o apurado em eventual diligência, além da desclassificação no processo licitatório, fica sujeita a licitante às penalidades cabíveis.

#### **7.4. QUALIFICAÇÃO ECONÔMICA E FINANCEIRA**

7.4.1. As exigências de qualificação econômica e financeira serão aquelas previstas no Edital.

#### **7.5. CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL e SICAF**

7.5.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda (comprovante emitido pela Receita Federal ou Certificado de Registro Cadastral – CRC, emitido pelo SICAF);

7.5.2. A inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

7.5.3. Provas de regularidade fiscal perante a Fazenda Municipal/Distrital do domicílio ou sede da arrematante;

7.5.4. Provas de regularidade fiscal perante a Fazenda Estadual/Distrital do domicílio ou sede da arrematante;

7.5.5. Provas de regularidade com a Fazenda Nacional, mediante a apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (SRFB) e Procuradoria Geral da Fazenda Nacional (PGFN);

7.5.6. Provas de regularidade perante o Fundo de Garantia por Tempo de Serviço - FGTS, fornecido pela Caixa Econômica Federal – CEF;

7.5.7. Provas de regularidade perante a Justiça do Trabalho;

7.5.8. Demonstrações de cumprimento do disposto no art. 7º, inc. XXXIII, da Constituição Federal.

#### **7.5.9. REQUISITOS DE HABILITAÇÃO SICAF**

7.5.9.1. A habilitação da arrematante cadastrada no SICAF será verificada por consulta on-line ao sistema, quanto aos documentos por ele abrangidos, e por meio da documentação complementar especificada neste edital.

7.5.9.2. Os documentos abrangidos pelo SICAF são os relativos à:

- habilitação jurídica, exceto comprovação de legitimidade para assinatura;
- de propostas e contratos de seu representante legal ou procurador;
- regularidade fiscal, social e trabalhista;
- qualificação econômico-financeira;
- qualificação técnica.

7.5.9.3. A arrematante não cadastrada no SICAF, ou com a documentação vencida/ausente no referido sistema, deverá apresentar o(s) documento(s) de habilitação nos prazos de envio da proposta recomposta.

#### **7.6. PARTICIPAÇÃO DE CONSÓRCIO E DE COOPERATIVA**

7.6.1. É vedada a participação de cooperativas devido à natureza do objeto da licitação. Também é vedada a participação de empresas reunidas em consórcio tendo em vista que as empresas atuantes no mercado têm, sozinhas, condições de fornecer o objeto da contratação e de suprir os requisitos do Termo de Referência, concorrendo entre si.

#### **7.7. SUSTENTABILIDADE**

7.7.1. O objeto ora contratado não apresenta riscos identificados de impactos ambientais.

7.7.2. Trata-se, resumidamente, de aquisição de solução de proteção de dados com

software, equipamentos de armazenamento e serviços correlacionados de implantação, capacitação, sustentação e horas técnicas especializadas adicionais.

7.7.3. No que tange aos equipamentos eles devem ser certificados por padrões de eficiência energética, como o Energy Star ou EPEAT, pode reduzir significativamente o consumo de energia.

7.7.4. Ademais, devem ser atendidos os seguintes requisitos de sustentabilidade:

- A Contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável, de acordo com o art. 225 da Constituição Federal de 1988, e ainda aplicar as normas técnicas da Associação Brasileira de Normas Técnicas – ABNT NBR, referente ao uso de materiais atóxicos, biodegradáveis e recicláveis;
- As embalagens devem ser fabricadas com materiais que propiciem a reutilização ou a reciclagem e devem ser restritas em volume e peso às dimensões requeridas à proteção do conteúdo e à comercialização do produto e recicladas, se a reutilização não for possível.

## **7.8. FORMALIZAÇÃO DA CONTRATAÇÃO**

7.8.1. As obrigações decorrentes desta contratação a serem firmadas entre o Tribunal de Justiça e a empresa vencedora serão formalizadas através de contrato, observando-se as condições estabelecidas neste Termo de Referência, da legislação vigente e da proposta apresentada.

7.8.2. A empresa vencedora do certame será regularmente convocada para assinar o contrato ou receber/retirar instrumento equivalente, dentro do prazo de (05) cinco dias úteis, sob pena de decair do direito à contratação, sem prejuízo das penalidades previstas em lei, neste termo, no instrumento convocatório e no contrato.

7.8.3. O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado durante o seu transcurso pela parte e desde que ocorra motivo justificado aceito pelo Tribunal de Justiça.

7.8.4. A recusa injustificada da empresa vencedora em assinar o contrato ou receber/retirar instrumento equivalente, dentro do prazo estabelecido neste Termo de Referência, caracteriza o descumprimento total da obrigação assumida, sujeitando-se às penalidades legalmente estabelecidas.

7.8.5. A empresa vencedora e/ou a empresa remanescente, se convocada, deverá comprovar as mesmas condições de habilitação consignadas no edital convocatório, como condição para celebração do contrato.

7.8.6. A assinatura de contratos e termos eletrônicos pode ser realizada também por meio eletrônico, nos termos do Decreto Judiciário nº 269/22 deste Tribunal de Justiça.

## **7.9. VISITA TÉCNICA**

7.9.1. Para melhor detalhamento dos serviços poderá ser agendada visita técnica nos datacenters com agendamento prévio no e-mail [monitoria@tjpr.jus.br](mailto:monitoria@tjpr.jus.br).

7.9.2. A vistoria nos datacenters tem como objetivo dar ciência da estrutura existente, fornecendo o conhecimento de aspectos que possam influir direta ou indiretamente a execução dos serviços.

7.9.3. Tendo em vista a faculdade da realização da vistoria, as licitantes não poderão alegar o desconhecimento das condições e grau de dificuldades existentes como justificativa para se eximirem das obrigações assumidas em decorrência do edital.

## **7.10. AMOSTRA**

7.10.1. Não será solicitada a apresentação de amostra, tão pouco a realização de prova de conceito para a contratação.

## **8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO**

8.1. O estudo para estabelecer a estimativa do valor da contratação encontra-se no documento de Estudos Técnicos Preliminares (SEI 13026686).

## 9. ADEQUAÇÃO ORÇAMENTÁRIA

9.1. A presente contratação estará prevista no Plano Anual de Contratações de Soluções de TIC para o exercício financeiro de 2026 vs. 1.3, apresentado no expediente administrativo SEI nº 0020597-40.2025.8.16.6000, o qual, foi apreciado pelo Comitê Gestor de Tecnologia da Informação e Comunicação (SEI nº 0033045-60.2016.8.16.6000 ata 12756002) e será apreciado pelo Comitê de Governança de Tecnologia da Informação e Comunicação na 2ª reunião de 2026 (SEI nº 0017736-81.2025.8.16.6000).

### ANEXOS

#### ANEXO 01 – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO / DEFINITIVO

TERMO DE RECEBIMENTO PROVISÓRIO/DEFINITIVO DE ENTREGA Fundamento Legal: art. 179 do Decreto estadual nº 10.086/2022. Pregão Eletrônico nº: XX/XXXX (SEI) Contrato: XXX/XXXX (REFERÊNCIA DOC. CONTRATO) Objeto: O quadro a seguir apresenta o detalhamento do objeto, seus quantitativos e valores.

Produto	Quantidade

Empresa Fornecedora/CNPJ: \_\_\_\_\_ Integrantes da Comissão para Recebimento do Objeto: Fiscal Técnico: Fiscal Demandante: Empenho emitido pelo FUNREJUS – Fundo de Reequipamento do Poder Judiciário: Empenho nº: XXXXX (DOC. REFERÊNCIA)

Valor: R\$ XXXXXX (EXTENSO)

Histórico: DESCRITIVO DO HITÓRICO DO EMPENHO. DATA DO RECEBIMENTO:

DD/MM/AAAA DATA DE EMISSÃO DA NF: DD/MM/AAAA NOTA FISCAL: XXXXX (DOC. REFERÊNCIA) VALOR: R\$ XXXXXX (EXTENSO)

Esta Comissão confere a subscrição e declara que foram recebidos em conformidade com as especificações do contrato celebrado entre este Tribunal e a referida empresa.

#### ANEXO 02 – MODELO DE TERMO DE CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE

Pelo presente instrumento, a empresa \_\_\_\_\_, com Sede à \_\_\_\_\_,  
inscrita no CNPJ/MF sob o número \_\_\_\_\_/\_\_\_\_\_-\_\_\_\_\_, doravante designada simplesmente  
RESPONSÁVEL, neste ato representada pelo Senhor(a) \_\_\_\_\_, RG nº \_\_\_\_\_  
e CPF nº \_\_\_\_\_, se compromete, por intermédio do  
presente TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE, a não divulgar sem autorização,  
utilizar para si, reproduzir ou dar conhecimento a terceiros das informações relativas a TJPR em especial  
das Plantas/Modelos fornecidos, enquanto material SIGILOSO pertencente à Tribunal de Justiça do Paraná,  
as quais devem ser conceituadas como SEGREDO DE NEGÓCIO, mediante as seguintes cláusulas e  
condições:

#### CLÁUSULA PRIMEIRA

A RESPONSÁVEL reconhece que tomou conhecimento de informações privadas do TJPR, que podem e  
devem ser conceituadas como segredo de negócio. Estas informações devem ser tratadas  
confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se  
incluindo os próprios empregados da RESPONSÁVEL, sem a expressa e escrita autorização de servidor  
autorizado do Tribunal de Justiça do Paraná.

Parágrafo Único - A RESPONSÁVEL determinará a todos os seus empregados, prepostos e prestadores de  
serviço que estejam diretas ou indiretamente envolvidos com a prestação de serviços objeto do Contrato, a  
observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas  
do presente instrumento sejam efetivamente observadas.

#### CLÁUSULA SEGUNDA

O RESPONSÁVEL, obriga-se, por si, seus sócios, administradores, funcionários, prepostos, contratados ou  
subcontratados e quaisquer outros que, através dos agentes da RESPONSÁVEL, tenham acesso a  
informações vinculadas ao presente, a manter o mais completo e absoluto sigilo com relação a toda e  
qualquer informação do TJPR a que tenham acesso.

Parágrafo 1º - O termo "informação" abrange toda informação escrita, verbal ou apresentada de outro modo  
tangível ou intangível, inclusive através de mídias digitais, especialmente relativas a informações  
administrativas, operacionais e técnicas, especificações e quaisquer outras informações técnicas,  
financeiras ou comerciais, relativas ao objeto do presente.

Parágrafo 2º - A RESPONSÁVEL poderá proceder ao fornecimento das informações confidenciais de que  
trata o presente quando exigidas por autoridade competente, mediante ordem judicial ou administrativa,  
obrigando-se, todavia, a imediatamente comunicar tal fato à Tribunal de Justiça do Paraná, por escrito,  
observando que as mesmas poderão ser liberadas consoante os termos da ordem judicial ou administrativa.

Parágrafo 3º - Os materiais, documentos e informações obtidos pela RESPONSÁVEL serão utilizados  
apenas com o propósito de formular proposta em licitação ou executar o serviço de reforma nas  
dependências do TJPR, caso reste vencedora da referida licitação.

Parágrafo 4º - Ao término da execução dos serviços, a RESPONSÁVEL se compromete a devolver à TJPR  
todos e quaisquer documentos, dados e materiais a que tenha tido acesso, inclusive todas e quaisquer  
cópias deles.

Parágrafo 5º - Todos os documentos e/ou informações necessários à execução dos serviços deverão ser  
solicitados sempre por e-mail criptografado utilizando recurso disponibilizado pelo TJPR ou deverão ser  
entregues ao TJPR, mediante relação e protocolo.

#### CLÁUSULA TERCEIRA

O não cumprimento de quaisquer cláusulas e condições deste TERMO implicará na responsabilidade civil e  
criminal dos que estiverem envolvidos na violação das regras de sigilo e confidencialidade de informações  
estabelecidas e formalizadas por meio deste TERMO.

Parágrafo Único - A infração de quaisquer disposições deste TERMO, estando ou não finalizado os serviços,  
em especial qualquer divulgação, utilização, transferência, cessão ou alienação, intencional ou não de  
qualquer informação confidencial, material, documentos e informações do TJPR ao mercado e/ou a outras  
pessoas físicas e/ou jurídicas, dará ensejo a indenizações por perdas e danos que porventura ao Tribunal de  
Justiça do Paraná e/ou seus administradores venham a sofrer em decorrência de tal falta, recaindo essas  
responsabilidades, exclusivamente, sobre os signatários deste compromisso, os quais serão apurados em  
juízo, na forma do art. 402 e seguintes do Código Civil.

#### CLÁUSULA QUARTA

O presente instrumento representa o consentimento integral da RESPONSÁVEL quanto à sua matéria e não  
poderá ser alterado sem o expresse e formal consentimento do TJPR. As disposições do presente termo  
vinculam os eventuais sucessores da RESPONSÁVEL, assim como quaisquer sociedades ou entidades,  
Contratadas ou ainda "afiliadas" à RESPONSÁVEL, nacionais ou estrangeiras, que venham a ter contato  
com as informações confidenciais, entendendo-se por "afiliadas" quaisquer sociedades controladoras,  
controladas ou que estejam sob o mesmo controle que a RESPONSÁVEL. O presente termo não poderá ser  
cedido sem o consentimento expresse do Tribunal de Justiça do Paraná.

Curitiba/PR, \_\_\_\_ de \_\_\_\_\_ de 20\_\_.

\_\_\_\_\_  
NOME DO SIGNATÁRIO

\_\_\_\_\_  
NOME DA EMPRESA



### **ANEXO 03 – TABELA DE PREÇOS**

O documento está disponível para download nos sites: [www.tjpr.jus.br/editais](http://www.tjpr.jus.br/editais) e [www.gov.br/compras](http://www.gov.br/compras).

### **ANEXO 04 – INSTRUMENTOS DE SOLICITAÇÃO DO(S) SERVIÇO(S)**

Após a assinatura do contrato, a CONTRATADA deverá indicar o preposto e os canais para solicitação e acompanhamento dos serviços, de acordo com critérios técnicos especificados neste Termo de Referência e em seus Anexos.

O prazo de garantia será de 60 (sessenta) meses, contados a partir do dia útil subsequente à data da emissão do termo de recebimento definitivo relativo aos itens do objeto. A garantia deverá atender, no mínimo, as seguintes condições:

- Prever assistência técnica on-site nas instalações do Tribunal de Justiça do Estado do Paraná ou remotamente, para solução de problemas de funcionamento e disponibilidade dos equipamentos e de esclarecimento de dúvidas relacionadas à instalação, configuração e uso dos produtos adquiridos;
- Prever manutenção e atualização dos produtos, mediante fornecimento e instalação de patches/firmwares/drivers, correções e versões de software para a aplicação de backup e para os equipamentos, independente da política de comercialização do fabricante;
- Englobar todas as funcionalidades suportadas pelos componentes da solução, incluindo hardware e software, independente de terem sido configurados anteriormente e da política de comercialização do fabricante;
- Prover central de abertura de chamados técnicos a partir de um número 0800 ou número local em Curitiba/PR, com disponibilidade 24 horas por dia, 7 dias por semana, e portal na internet. No momento de abertura do chamado, deverá ser fornecido ao TJPR um número único de identificação. Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema da CONTRATADA para controle de chamados. O acesso a esse sistema deverá estar disponível ao Tribunal quando solicitado. Além disso, os chamados abertos somente poderão ser fechados após autorização do TJPR;
- Qualquer chamado fechado, sem anuência do TJPR ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas;

Em relação do serviço contido Item 7, por se tratar de contratação por pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços, e assim não configura como contratação com dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho, durante a fase de execução do contrato:

a) A CONTRATADA deverá disponibilizar profissional(is) com perfil de Analista de Backup Pleno, vinculados a base salarial dos profissionais previstos na planilha de custos e formação de preços constante da proposta vencedora da licitação.

b) A fiscalização do contrato verificará o alcance do objetivo do serviço prestado, a efetiva disponibilização dos perfis profissionais mínimos previsto, a qualidade dos produtos/resultados entregues e o prazo de atendimento conforme critérios de aceitação e níveis mínimos de serviço estabelecidos.

c) A CONTRATADA possui total gestão sobre a equipe do contrato, podendo realizar alterações na quantidade dos profissionais envolvidos na prestação do serviço, bem como decidir sobre a alocação destes profissionais entre atividades de múltiplos contratos, desde que sejam observados os limites de atuação previstos para cada perfil profissional no catálogo de serviços.

O fluxo de controle dos serviços técnicos especializados referente ao processo de gerenciamento das horas técnicas sob demanda contidas no - Item 8 é formado pelos seguintes componentes:

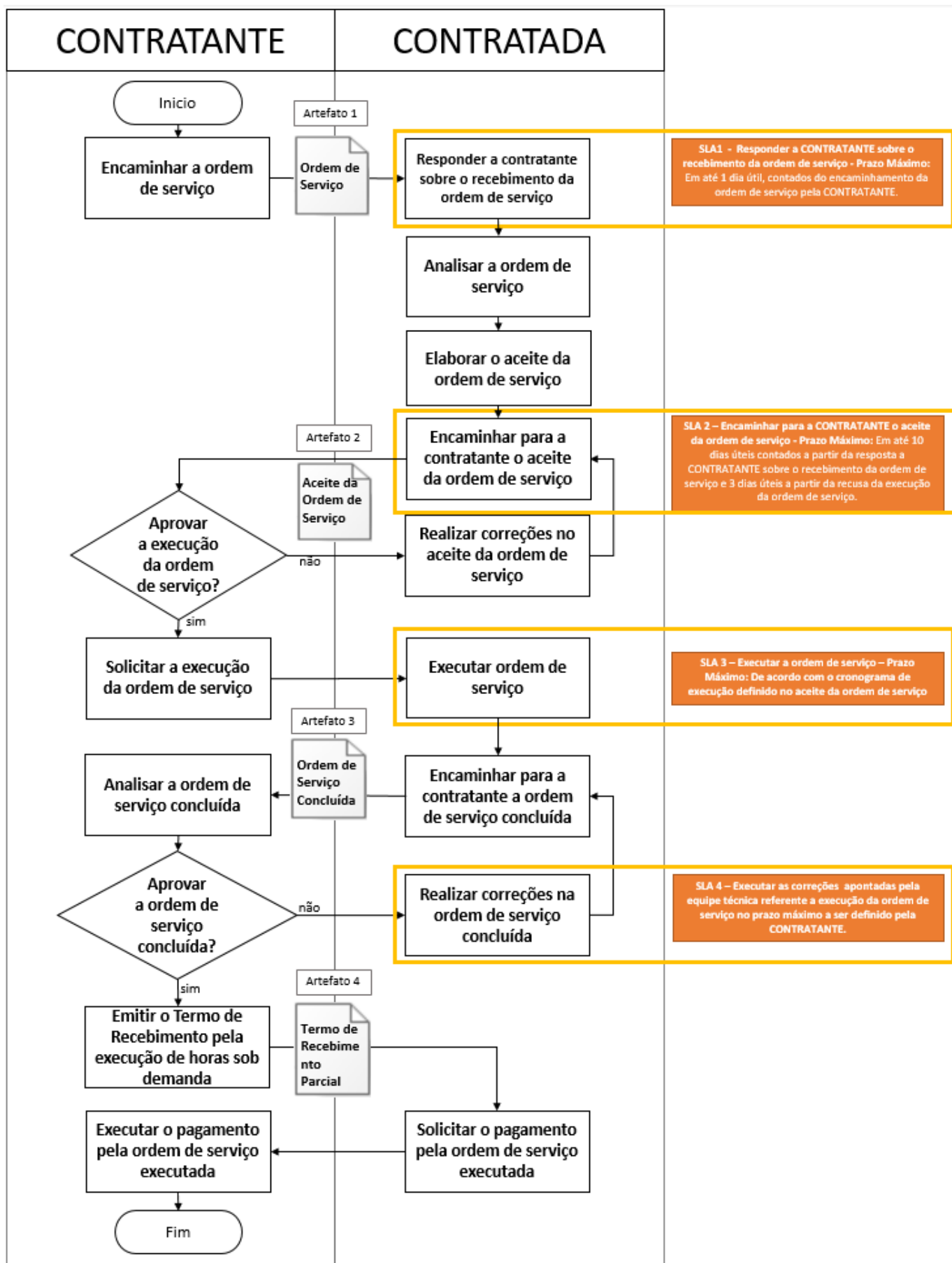


Figura 1: Fluxo de solicitação de serviços sob demanda

**Atores/Responsáveis/Partes:**

CONTRATANTE: o Tribunal de Justiça do Estado do Paraná

CONTRATADA: a empresa Contratada.

## **Atividades**

1. Encaminhar a ordem de serviço
2. Responder o CONTRATANTE sobre o recebimento da ordem de serviço
3. Analisar a ordem de serviço
4. Elaborar o aceite da ordem de serviço
5. Encaminhar para o CONTRATANTE o aceite da ordem de serviço
6. Realizar correções no aceite da ordem de serviço
7. Aprovar a execução da ordem de serviço?
8. Solicitar a execução da ordem de serviço
9. Executar ordem de serviço
10. Solicitar a alteração da quantidade de horas técnicas, créditos, valor ou do cronograma de execução?
11. Aprovar a alteração da quantidade de horas técnicas, créditos, valor ou do cronograma de execução?
12. Informar a aprovação da alteração da quantidade de horas técnicas, créditos, valor ou do cronograma de execução.
13. Encaminhar para o CONTRATANTE a ordem de serviço concluída
14. Analisar a ordem de serviço concluída
15. Aprovar a ordem de serviço concluída?
16. Realizar correções na ordem de serviço concluída
17. Emitir o Termo de Recebimento relativo a horas técnicas sob demanda pela Execução da Ordem de Serviço
18. Encaminhar para a CONTRATADA o Termo de Recebimento relativo a horas técnicas sob demanda pela Execução da Ordem de Serviço
19. Solicitar o pagamento pela ordem de serviço executada.
20. Efetuar o pagamento pela ordem de serviço executada.

## **Artefatos:**

1. Os artefatos definem requisitos mínimos esperados para cada modelo de ordem de serviço previsto no fluxo de controle dos serviços técnicos especializados, os quais seguem:

### **Ordem de Serviço (Artefato 1)**

1. Identificação da ordem de serviço (documento registrado no SEI);
2. Número do contrato;
3. Nome do gestor do contrato;
4. Nome do fiscal técnico do contrato;
5. Nome da equipe técnica;
6. Nome do demandante da ordem de serviço;
7. Data de início sugerida para a execução da ordem de serviço;
8. Data de término sugerida para a execução da ordem de serviço;
9. Estimativa da quantidade de horas técnicas necessária para a execução da ordem de serviço;
10. Especificações da ordem de serviço;
12. Especificação dos artefatos da ordem de serviço;
13. Data da ordem de serviço;
14. Assinatura do fiscal técnico do contrato;
15. Assinatura do gestor do contrato;
16. Assinatura do demandante;

### **Aceite da ordem de serviço (Artefato 2)**

1. Identificação da ordem de serviço (documento registrado no SEI);
2. Nome do técnico responsável pelo aceite da ordem de serviço;
3. Identificação do aceite da ordem de serviço;
4. Quantidade de horas técnicas necessárias para a execução da ordem de serviço;
5. Quantidade de horas para a execução da ordem de serviço;
6. Especificação da execução da ordem de serviço;
7. Especificação dos artefatos da execução da ordem de serviço;

8. Cronograma da execução, que deverá conter no mínimo:
9. Data de início;
10. Data de término;
11. Dependendo do nível de complexidade da execução da ordem de serviço, deverão ser definidos os marcos de entregas parciais e suas respectivas:
12. Data de início do marco de entrega parcial;
13. Data de término do marco de entrega parcial.
14. Data do aceite da ordem de serviço;
15. Assinatura do técnico responsável pelo aceite da ordem de serviço

### **Ordem de serviço concluída (Artefato 3)**

1. Identificação da ordem de serviço (documento registrado no SEI);
2. Identificação da ordem de serviço concluída;
3. Nome do responsável técnico que realizou a execução da ordem de serviço;
4. Quantidade de horas técnicas necessárias para a execução da ordem de serviço;
5. Valor total baseado na quantidade de horas técnicas necessárias para execução da ordem de serviço;
6. O cronograma de execução definido no aceite da ordem de serviço;
7. A descrição dos serviços técnicos especializados realizados na execução da ordem de serviço;
8. Os artefatos desenvolvidos durante a execução da ordem de serviço.

9. Data da ordem de serviço concluída

10. Assinatura do responsável técnico que realizou a execução da ordem de serviço

### **Termo de Recebimento relativo a horas técnicas sob demanda pela Execução da Ordem de Serviço (Artefato 4)**

1. Identificação da ordem de serviço aprovada (documento registrado no SEI);
2. Identificação da ordem de serviço (documento registrado no SEI);
3. Número do contrato;
4. Nome do fiscal técnico do contrato;
5. Nome do gestor do contrato;
6. Nome do demandante;
7. Nome do responsável técnico que realizou a execução da ordem de serviço;
8. Quantidade de horas técnicas necessárias para a execução da ordem de serviço;
9. Valor cobrado para a execução da ordem de serviço;
10. Data da ordem de serviço concluída
11. Avaliação do cumprimento do cronograma de execução definido no aceite da ordem de serviço;
12. Data da ordem de serviço aprovada;
13. Assinatura do fiscal técnico do contrato;
14. Assinatura do gestor do contrato;
15. Assinatura do demandante;

## **ANEXO 05 – TERMOS E DEFINIÇÕES**

Appliance	Um appliance de backup é um dispositivo de hardware dedicado, integrado com software especializado, projetado para realizar funções de backup, recuperação de dados e, muitas vezes, arquivamento e replicação de dados.
Backups	É o processo de criar cópias de dados importantes para garantir que eles possam ser restaurados em caso de perda, corrupção, ou outro tipo de falha.
Calendário oficial do TJPR	Disponível no endereço eletrônico <a href="http://www.tjpr.jus.br/calendario">http://www.tjpr.jus.br/calendario</a>
Chamado ou Chamado Técnico	Toda e qualquer manifestação do CONTRATANTE para a CONTRATADA relativo a dúvidas ou falhas do objeto contratado.
CBO	Classificação Brasileira de Ocupações
Cluster	Em processamento de dados, um "cluster" refere-se a um grupo de computadores interconectados que trabalham juntos para processar tarefas de forma coordenada.

CONTRATADA	A empresa vencedora do processo licitatório e responsável pelo objeto será denominada simplesmente de CONTRATADA.
Core(s)	Na computação, um "core" (núcleo, em português) refere-se a uma unidade de processamento central em um processador (CPU).
CPU	Significa Central Processing Unit ou Unidade Central de Processamento" em inglês, e refere-se ao principal componente de um computador que executa instruções de programas e coordena as atividades dos outros componentes do sistema. Um processador é composto por um ou mais núcleos (ou cores).
Data center	É uma instalação física centralizada onde encontram-se servidores de processamento de dados, equipamentos de rede, equipamentos de armazenamento de TIC que suportam às aplicações e serviços do TJPR.
End of Life	Fim de vida, sinônimo de End of Support;
End of Support	Fim do suporte pelo fabricante;
Fibre Channel	ou FC, é uma tecnologia de comunicação de alta velocidade que é utilizada em armazenamento de dados em rede.
HBA Adapter	Host Bus Adapter - Adaptador de host, controlador de host ou adaptador de barramento de host conecta um servidor a outros dispositivos de rede ou de armazenamento.
HDD	HDD (Hard Disk Drive) é um dispositivo de armazenamento de dados que utiliza discos magnéticos rotativos para ler e gravar informações. É composto por uma série de pratos (discos) que giram em alta velocidade, com cabeças de leitura/gravação posicionadas sobre eles para acessar os dados. O HDD é um dos métodos mais antigos e amplamente utilizados para armazenamento em massa.
Horário Regimental do TJPR	Período compreendido entre 12 (doze) e 19 (dezenove) horas, de segunda-feira a sexta-feira, excluídos os feriados considerando o calendário oficial do TJPR.
Host	Como é chamado o servidor de processamento de dados.
Incidente	Corresponde a uma interrupção (ou falha) não planejada de um serviço de TIC ou a uma redução na qualidade do serviço.
IOPS	(Input/Output Operations Per Second) - Operações de entrada e saída por segundo.
iSCSI	Internet Small Computer System Interface - protocolo de transporte que transporta comandos SCSI entre um computador anfitrião e um dispositivo de destino.
Jobs	Refere-se a uma tarefa ou processo automatizado que é configurado para realizar backups de dados.
Kubernetes	De forma simples, o Kubernetes automatiza o processo de implantação, escalonamento e gerenciamento das aplicações em contêineres, permitindo que as equipes de desenvolvimento se concentrem em escrever código e os operadores de sistemas possam lidar com a infraestrutura. Ele também ajuda a garantir que os aplicativos estejam sempre disponíveis, sejam executados de forma consistente e possam ser facilmente escalonados para atender às demandas de tráfego.
LAN	Local Area Network, Rede de área local - Uma rede de área local em computação consiste em uma rede de computadores utilizada na interconexão de equipamentos processadores, cuja finalidade é a troca de dados;
LUN	Logical Unit Numbers, Número de Unidade Lógica - é o número usado para identificar uma unidade lógica de um dispositivo endereçável através do protocolo SCSI ou protocolos SAN, que encapsulam SCSI, como Fibre Channel ou iSCSI.
NAS	Network-Attached Storage, Armazenamento ligado à rede - é um dispositivo dedicado ao armazenamento arquivos em rede, provendo acesso homogêneo aos dados para os clientes desta rede.
Nuvem privada	É um modelo de computação em nuvem onde os recursos de computação são dedicados exclusivamente a uma única organização. Uma nuvem privada pode ser implementada dentro das instalações da organização (on-premises), utilizando seus próprios servidores e infraestrutura de rede

Nuvem pública	É um modelo de computação onde os recursos de computação são compartilhados entre várias organizações e usuários. Os provedores de nuvem pública são responsáveis por gerenciar e manter a infraestrutura subjacente, como servidores, armazenamento e redes.
NVMe	NVMe (Non-Volatile Memory Express) é um protocolo de comunicação e armazenamento criado para acessar dispositivos de armazenamento não volátil, como SSDs (Solid State Drives), por meio da interface PCIe (Peripheral Component Interconnect Express). Ele foi projetado para substituir os antigos protocolos como o AHCI (Advanced Host Controller Interface), que foi otimizado para discos rígidos mecânicos (HDDs), e não para os SSDs, que são muito mais rápidos.
Object Storage	Object storage ou armazenamento objeto é um método de armazenamento de dados que organiza informações como objetos independentes, cada um com dados, metadados e um identificador único, permitindo escalabilidade e eficiência na gestão de grandes volumes de dados.
Offsite	Área de armazenamento localizado fora do local físico principal.
On-premises	Este termo refere-se a um modelo de infraestrutura de tecnologia da informação onde os servidores, sistemas e aplicativos são instalados e executados localmente nas instalações da organização.
OS	Ordem de Serviço
Petabyte - PB	1 Petabyte é igual a $2^{50}$ bytes, ou 1.125.899.906.842.624 bytes.
PM	Gerente de Projetos – Project Manager.
RAID	Redundant Array of Independent Disks, Matriz Redundante de Discos Independentes - é um meio de se criar um subsistema de armazenamento composto por vários discos individuais, com a finalidade de ganhar segurança, por meio da redundância de dados, e desempenho.
Resolução Nº 468/2022	Resolução Nº 468/2022 do Conselho Nacional de Justiça, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça
Restore	Refere-se à ação de recuperar dados a partir de um backup previamente realizado.
SAN	Storage Area Network, Rede de área de armazenamento - Rede de área de armazenamento é uma rede destinada exclusivamente a armazenar dados, ou seja, o conceito de armazenamento de dados em rede;
Scripts	Scripts são arquivos contendo um conjunto de instruções ou comandos que são interpretados ou executados sequencialmente por um programa ou ambiente de execução específico.
SCSI	Small Computer System Interface - é uma tecnologia que permite ao usuário conectar uma larga gama de periféricos, tais como discos rígidos, unidades CD-ROM.
Servidor de processamento de dados	É um recurso de hardware dentro de um parque tecnológico ou data center, capaz de processar aplicações e serviços de tecnologia da informação.
Servidor Virtual ou VM	É o processo de virtualizar os recursos de hardware de um servidor de processamento de dados físico. Desta forma é possível disponibilizar os seus recursos de hardware entre um ou diversos servidores virtuais de forma compartilhada. VM vem do termo em inglês Virtual Machine.
SETI	Secretaria de Tecnologia da Informação será denominado simplesmente de “SETI” e seu endereço oficial é Rua Álvaro Ramos nº 157, 1º andar, Centro Cívico, Curitiba – Paraná.
Solução de TIC	de acordo com o Art. 2º, Resolução nº 468/2022 do CNJ, todos os bens e/ou serviços de TI que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou, exceto materiais de consumo considerados pela área administrativa do órgão

SSD	SSD (Solid State Drive) é um dispositivo de armazenamento de dados que utiliza memória flash (geralmente do tipo NAND) para armazenar e acessar informações de forma rápida e eficiente, sem partes móveis, ao contrário dos discos rígidos tradicionais (HDDs). Os SSDs são amplamente utilizados por sua velocidade superior, confiabilidade e menor consumo de energia.
Storage	Equipamento de armazenamento de dados;
Storage	Um dispositivo ou repositório responsável pelo armazenamento dos dados de uma corporação.
Switches	Dispositivos de interconexão de dispositivos de atuação em redes telemáticas.
Tempo de Solução (TS)	Período compreendido entre o horário de comunicação do chamado feito pela CONTRATANTE, e o horário do término do serviço, restabelecendo o serviço ou disponibilizando uma solução de contorno.
Terabyte - TB	1 Terabytes é igual a $2^{40}$ bytes, ou 1.099.511.627.776 bytes.
Throughput	Taxa de transferência, podendo ser chamado também de índice de vazão média, throughput é a métrica que mede a capacidade de entrega em um ciclo de tempo.
TI	a Tecnologia da Informação será denominada simplesmente de "TI"
TIC	Tecnologia da Informação e Comunicação.
TJPR	Tribunal de Justiça do Estado do Paraná.
TR	Termo de Referência
Virtualização	É o processo de segmentar os recursos de um servidor de processamento de dados físico e compartilhar estes recursos entre servidores virtuais únicos e isolados, possibilitando a execução de seus próprios sistemas operacionais de forma independente.

## ANEXO 06 – PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

Identificação da Licitação					
Nº do Processo					
Nº da Licitação					
Nome da Empresa					
CNPJ					
GRUPO XX - <descrição do grupo>					
ITEM XX - <descrição do Item>					
Componentes de Custo de Pessoal					
Identificação do Perfil Profissional	Salário (S)	Fator K (K)	Custo total por perfil (CT= S x K)	Qtde. profissionais por perfil (Q)	Custo Mensal por Perfil (CM = CT x Q)
Subtotal componentes de custo de Pessoal					
Demais Componentes de Custo					
Descrição	Memória de Cálculo / Justificativa			Valor Mensal	

Custos com software		
Custos com recursos de computação		
Custos com equipamentos		
Custos com serviços de informações		
Outros custos (especificar)		
Subtotal Demais componentes de custo		
Componentes de Preço (não compreendidos na composição do fator K)		
Descrição		Valor Mensal
Elementos Comerciais (Fatores/Ajustes Comerciais)		
Cobertura Tributária		
Outros componentes (especificar)		
Subtotal componentes de preço		
Total Mensal:		
Valor Total do [item/grupo]:		
[Valor mensal x quantidade de meses previstos para contratação]		

## ANEXO 07 – REQUISITOS TÉCNICOS

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) 2	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) 3
1	SOFTWARE DE BACKUP E SERVIDORES PARA PROTEÇÃO DE INFRAESTRUTURA			
1.1	Características Gerais			
	O software de proteção de dados deverá possuir licenças suficientes para cobrir 800 máquinas virtuais, 50 worknodes Kubernetes/Tanzu, 700 TB de armazenamento NAS ou S3 e uma volumetria de frontend de 4 (quatro) PB (Petabytes). Para garantir o licenciamento adequado, o PROPONENTE deverá seguir os requisitos descritos a seguir: - Caso o software de proteção de dados tenha um licenciamento específico para máquinas virtuais, considerar a quantidade de 800 (oitocentas) VMs, para fins de			



ITEM 1.1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.1.1	<p>- Caso o software de proteção de dados tenha um licenciamento específico para backup do frontend de NAS (CIFS ou NFS) ou S3, considerar a o valor mínimo de 700 (setecentos) TB (Terabytes) para estes tipos de armazenamento.</p> <p>- Caso o software de proteção de dados tenha licenciamento pela volumetria de frontend total, considerar o valor de 4 (quatro) PB (Petabytes) para este tipo de armazenamento.</p> <p>- Caso o software de proteção de dados tenha um licenciamento específico para backup do ambiente containerizado Kubernetes/Tanzu, o licenciamento deverá prover proteção para 50 (cinquenta) nós (worker nodes), sem limitação da quantidade de instâncias, aplicações ou namespaces protegidos, quer sejam máquinas físicas ou virtuais, ou uma volumetria líquida de no mínimo de 700 (setecentos) TB (Terabytes) de frontend.</p> <p>- Caso o software de proteção de dados tenha um licenciamento por sockets de processamento físico, considerar a o valor mínimo de 148 (cento e quarenta e oito) sockets físicos.</p> <p>- Caso o software de proteção de dados necessite de um licenciamento específico para efetuar a proteção de equipamentos de processamento de dados, considerar o valor mínimo de 100 (cem) servidores físicos.</p> <p>- Independente da métrica de licenciamento utilizada (Instância ou Capacidade), o proponente deve garantir que todos os recursos de segurança avançada, orquestração e conformidade disponíveis na plataforma estejam licenciados para a totalidade da volumetria e objetos listados, dentro das funcionalidades nativas e disponíveis de cada componente do software ofertado, sem custos extras para o contratante na necessidade de aquisição de módulos ou licenças adicionais.</p>			
1.1.2	O licenciamento fornecido deverá ser por subscrição.			
1.1.3	O licenciamento e o software de proteção de dados ofertado deverão proteger ambientes virtuais com Hyper-V, Nutanix AHV, VMware, Red Hat Virtualization e Oracle Linux Virtualization Manager. Proteger também de forma nativa e integrada usando as APIs os ambientes de Cloud Amazon AWS, Microsoft Azure e Google Cloud (GCP).			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.4	Para Máquinas virtuais, servidores físicos e instancias de computacionais em cloud o software de proteção de dados não deverá apresentar limitações quanto a capacidade protegida (Frontend) ou volume de dados armazenados no Backup (Back-End). Caso o software de proteção de dados tenha licenciamento baseado em volume de frontend, este não deverá ter limite de máquinas virtuais, servidores físicos e instancias computacionais on premisses ou em cloud protegidas.			
1.1.5	O software de proteção de dados ofertado deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do Fabricante, ou com end-of-life ou end-of-support anunciado.			
1.1.6	O software de proteção de dados deverá prover licenciamento que englobe todas as funcionalidades e requisitos elencados neste Termo de Referência, independentemente de qualquer quantidade de utilização do referido serviço, sem nenhum Tipo de cobrança adicional para a CONTRATANTE.			
1.1.7	O software de proteção de dados ofertado deverá englobar todos os módulos de software que o compõe pertencentes ao mesmo fabricante, não sendo aceitas composições de softwares de fabricantes distintos para o atendimento as especificações.			
1.1.8	O licenciamento ofertado deverá ser fornecido com garantia, incluindo suporte técnico e atualização de releases. As licenças deverão estar no nome da CONTRATANTE.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.9	<p>O suporte técnico deve ser na modalidade 24x7x365 e prestado diretamente pelo FABRICANTE, seguindo o SLA de atendimento conforme a criticidade abaixo:</p> <ul style="list-style-type: none"><li>- Grave - Prazo para início de atendimento de no máximo 1 hora, alguns exemplos: Todas as tarefas de backup e replicação estão em falha; Dados de produção ausentes que precisam ser restaurados urgentemente usando a solução de backup.</li><li>- Alta - Prazo para início de atendimento de no máximo 3 horas, alguns exemplos: Impactando negativamente várias tarefas de backup primárias, mas os sistemas de produção não estão inativos; as operações de produção são afetadas, mas o impacto é limitado.</li><li>- Média - Prazo para início de atendimento de no máximo 8 horas, alguns exemplos: Falhas limitadas nas tarefas de backup primárias ou falhas nas tarefas de backup secundárias; Software de backup com problemas ou dúvidas que prejudiquem a operação do software, mas que não interrompam o acesso aos serviços.</li><li>- Baixa - Prazo para início de atendimento de no máximo 24 horas, alguns exemplos: Pequeno problema ou dúvida que não afeta a função do produto e pode ser facilmente contornado.</li></ul>			
1.1.10	<p>O software de proteção de dados ofertado não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante.</p>			
1.1.11	<p>O software de proteção de dados deverá permitir a escalabilidade horizontal, de modo a suportar a instalação e configuração de servidores proxies físicos ou virtuais, servidores de repositório, de mídia ou de gerenciamento em quantidade ilimitada, sem restrições de crescimento.</p>			
1.1.12	<p>O software de proteção de dados deverá incluir funcionalidades de proteção (backup) de todas as cargas de trabalho especificadas nesse termo de referência e replicação de máquinas virtuais VMware e Hyper-V, integradas em uma única solução, incluindo a possibilidade de realizar um failover para o site de destino e um failback para o site original, considerando apenas o diferencial (delta) dos dados alterados durante essa operação.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.13	O software de proteção de dados não deverá necessitar de instalação manual de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.			
1.1.14	O software deve possuir todas as licenças necessárias para atividades de backup, recuperação, capacidade de replicação contínua de dados (CDP), bem como orquestração nativa de planos de recuperação de desastres (DR), incluindo testes automatizados de restauração em ambiente isolado, verificação de integridade de aplicações e geração de relatórios de conformidade (RPO/RTO) de forma automatizada.			
1.1.15	O software de proteção de dados deverá possibilitar a proteção de dados de Máquinas Virtuais operando de modo integrado e utilizando APIs nativas de backups dos hypervisores, sem a necessidade do uso de agentes.			
1.1.16	O software de proteção de dados deverá oferecer suporte para VMware vCloud Diretor com visibilidade integrada da infraestrutura de vCD no console de backup, tornando o backup e os atributos de metadados associados a vApps e VMs, permitindo a recuperação diretamente para o vCD e permitindo o autogerenciamento de tarefas de backup e recuperação gerenciadas pelo tenant.			
1.1.17	O software de proteção de dados deverá permitir a criação de tarefas de backup, de modo a agendar e automatizar os processos, permitindo a criação de diferentes políticas conforme as necessidades da CONTRATANTE.			
1.1.18	O software de proteção de dados deverá permitir adicionar automaticamente as máquinas virtuais com VMware vSphere ou Microsoft Hyper-V, descobertas em rotinas de backup, com capacidade de realizar filtros avançados com critérios que incluam pelo menos: a.Host; b.Cluster; c.Resource Pool (em ambientes VMware); d.Pastas (em ambientes VMware); e.VM Tags (em ambientes VMware); f.Datastore; g.vApp (em ambientes VMware);			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.19	<p>O software de proteção de dados deverá suportar os métodos de backup Full e Incremental com pelo menos os seguintes requisitos:</p> <p>Possuir no método Incremental, suporte ao modo Incremental Forever, ou seja, o backup deve consistir em apenas de um backup Full e todos os demais incrementais até o término do período de retenção.</p> <p>Permitir a geração de cópias de longa retenção full, tanto no modo ativo - executando um novo backup Full no cliente quanto no modo sintético utilizando os backups já salvos anteriormente.</p> <p>Permitir o agendamento para geração automática destas cópias.</p>			
1.1.20	<p>O software de proteção de dados deverá suportar a política de retenção de longo prazo utilizando o recurso GFS (Grandfather-Father-Son), onde deverá ser possível estabelecer políticas de retenção para backups semanais, mensais e anuais na mesma tarefa de backup.</p>			
1.1.21	<p>O software de proteção de dados deverá ser capaz de fazer backups incrementais utilizando a tecnologia de rastreamento de blocos de disco modificados (Changed Block Tracking – CBT e Resilient Block Tracking) minimizando o tempo de backup e permitindo que uma cópia de segurança (backup) seja realizada de maneira mais frequente.</p>			
1.1.22	<p>O software de proteção de dados deverá possuir tecnologia de deduplicação e compressão para obter uma economia de espaço de armazenamento para backups sem a necessidade de hardware específico para esse fim.</p>			
1.1.23	<p>O software de proteção de dados deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.</p>			
1.1.24	<p>O software de proteção de dados deverá possuir módulo nativo de criptografia AES (Advanced Encryption Standard) 256 bits.</p>			
1.1.25	<p>O software de proteção de dados deverá possuir nativamente funcionalidade que permita a implementação de imutabilidade de dados, armazenamento WORM ou similares, com o objetivo de prover proteção contra a alteração e exclusão dentro do repositório de dados;</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.26	O software de proteção de dados deverá possuir trabalhos de cópia de backup com a possibilidade de copiar um backup existente para um outro repositório, com políticas de retenção específicas para a cópia, não dependendo da política de retenção do backup que originou a cópia. Deverá ser possível realizar a cópia dos backups entre diferentes Tipos de repositórios, por exemplo, de um repositório Linux para um repositório Windows, ou de um repositório NFS para um Appliance de Backup.			
1.1.27	O software de proteção de dados deverá realizar backups em disco, e deverá suportar diversos tipos de repositório, não dependendo de hardware específico para armazenamento de backups, permitindo que sejam utilizados para repositório ao menos os seguintes dispositivos: Servidores Físicos e virtuais Linux e Windows com armazenamento local ou utilizando volumes de um storage SAN; Compartilhamentos de rede NFS e CIFS(SMB); Appliances de Backup; Storages do Tipo Objeto (S3).			
1.1.28	Suportar deduplicação a nível de blocos, em volumes apresentados através de DAS (Direct Attached Storage) e SAN (Storage Area Network) e em Compartilhamento de rede NAS, via protocolos SMB e NFS.			
1.1.29	Suportar deduplicação de dados na origem (source deduplication), de forma que sejam enviados apenas novos blocos de dados criados e/ou modificados a partir da última cópia de segurança.			
1.1.30	Permitir armazenar cada máquina virtual em um arquivo de backup distinto ou permitir fluxos de gravação em paralelo ao armazenar cópias de segurança em appliances de backup, suportando no mínimo os seguintes modelos de equipamento: Dell EMC Data Domain, Exagrid, HPE StoreOnce e Quantum DXi. A comprovação deste item poderá ser realizada por meio de documentação oficial ou matriz de compatibilidade emitida pelo fabricante do software de backup e/ou pelo fabricante do appliance.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.31	<p>A solução de proteção de dados deve contemplar, de forma nativa e integrada, os seguintes recursos avançados de segurança e resiliência cibernética:</p> <ul style="list-style-type: none"><li>- Capacidade de realizar varreduras automáticas e/ou sob demanda em dados de backup já realizados, utilizando mecanismos baseados em assinaturas (Threat Scan ou equivalente), análise de entropia, identificação de arquivos modificados/encryptados e detecção de ferramentas legítimas utilizadas de forma suspeita para execução de ataques (indicators of Compromise ou equivalente), permitindo análise pré-restauração e ações preventivas caso uma ameaça seja identificada.</li><li>- Ser compatível com restauração em ambiente isolado (sandbox/cleanroom) para testes de recuperação, análises forenses e validação de integridade dos dados, sem risco para o ambiente de produção.</li><li>- Geração automática de alertas e relatórios detalhados sobre os mecanismos de detecção disponíveis na plataforma como por exemplo, detecção de criptografia, atividades suspeitas, varredura de malware e inclusive deve possibilitar integração com sistemas de monitoramento e SIEM.</li><li>- Proteção de imutabilidade dos dados de backup, de forma nativa, sem dependência de scripts, contemplando suporte a storage compatível com WORM ou repositórios protegidos contra alteração/exclusão durante o período de retenção.</li><li>- Garantia de recuperação dos dados mesmo em caso de comprometimento do catálogo ou do servidor principal, ou por meio de importação dos backups protegidos/imutáveis, desde que tais backups sejam autossuficientes e não dependam do catálogo no servidor original.</li></ul>			
1.1.32	<p>O software de proteção de dados deverá suportar repositórios com aumento de escala ilimitado para o armazenamento dos Backups.</p>			
1.1.33	<p>O software de proteção de dados deverá permitir a adição de novos repositórios de backup ao Repositório de Escala em qualquer tempo, permitindo a expansão da capacidade de armazenamento.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.34	O software de proteção de dados deverá permitir a remoção de um membro de um repositório de escala ilimitada em qualquer tempo. O software de proteção de dados deverá prover meios para mover os dados de um repositório para o outro se o Administrador desejar removê-lo.			
1.1.35	O software de proteção de dados deve permitir a redistribuição dos arquivos de backup (rebalance) entre os membros do repositório de backup, caso a solução possua esse tipo de característica de implementação, permitindo assim otimizar a utilização de todos os recursos de armazenamento. Caso a solução não possua esse tipo de característica, não devem existir limitações relacionadas a expansão de repositórios de backup.			
1.1.36	Deverá ser possível colocar um dos membros em modo de serviço ou implementar funções similares de movimentação e provisionamento de repositórios de backup, de modo a permitir atualizações e manutenções sem indisponibilizar completamente o repositório de backup.			
1.1.37	Possuir capacidade de gerenciar software de snapshot de storages de outros fabricantes, suportando ao menos os equipamentos Dell Unity e PowerMax, IBM FlashSystem e Storwize, NetApp ONTAP, HPE 3PAR/Primera/Alletra e Pure Storage FlashArray, com o intuito de automatizar o processo de agendamento de cópias "snapshot" e montagem no servidor de backup "off-host";			
1.1.38	Deve possuir mecanismos que automatizem a orquestração e recuperação a partir de snapshots do storage de produção, com suporte a recuperação instantânea de máquinas virtuais e recuperação granular de arquivos e bases de dados (SQL Server, Oracle e PostgreSQL) diretamente desses snapshots de storages compatíveis ou implementar funcionalidades de recuperação granular a nível de máquinas virtuais ou datastore para os casos em que não existir compatibilidade de snapshot.			



**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.39	O software de proteção de dados deverá fornecer meios para que os backups armazenados no repositório de backup local sejam automaticamente copiados para um repositório em nuvem, tão logo seja criado, suportando ao menos os seguintes provedores: Amazon AWS S3, Microsoft Azure Blob Storage, IBM Cloud Object Storage, Google Cloud Object Storage e demais produtos compatíveis com S3 (Simple Storage Service).			
1.1.40	O uso de object storage como repositório de backup não deve limitar as capacidades de recuperação, tais como: recuperação granular e checagem da integridade dos backups.			
1.1.41	O software de proteção de dados deverá suportar repositórios de backup do tipo S3 objeto com capacidade de imutabilidade, de modo que os arquivos de backup não possam ser alterados ou excluídos por um determinado período, prevenindo assim a corrupção dos dados através de malware.			
1.1.42	O software de proteção de dados deverá ainda possibilitar a movimentação das cadeias de backup antigas de repositórios em disco para storages do tipo objeto ou repositórios em nuvem, conforme estabelecido em política.			
1.1.43	Quando integrado ao armazenamento em nuvem pública, ele deve ser autossuficiente e não depender de qualquer catálogo gravado localmente (On-Premises), para isso a solução deve possuir replicação específica e segura do catálogo em nuvem pública ou realizar essa produção de forma integrada, desde que sejam implementadas políticas de segurança para ele, permitindo, em caso de desastre, a recuperação completa dos arquivos armazenados na nuvem pública.			
1.1.44	O software de proteção de dados deverá suportar backups em fita, incluindo o suporte a bibliotecas com múltiplos drives e VTLs.			
1.1.45	O software de proteção de dados deverá possibilitar o envio dos backups já criados no repositório de disco para a fita.			
1.1.46	O software de proteção de dados deverá suportar mídia de fita LTO (Linear Tape-open) 3 e superiores.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.47	O software de proteção de dados deverá possuir a capacidade de definir grupos de fitas magnéticas a serem usadas na mesma sessão de armazenamento em fita (Pool de Mídia) para maximizar a taxa de transferência e a velocidade de transferência.			
1.1.48	O software de proteção de dados deverá suportar Pools de fita do Tipo GFS Grandfather-Father-Son.			
1.1.49	O software de proteção de dados deverá suportar WORM (Write Once Read Many) para arquivamento de Backups em Fita.			
1.1.50	O software de proteção de dados deverá ter a capacidade de processar o envio de dados em várias unidades de fita, em paralelo para maximizar a largura de banda e minimizar o tempo de transferência.			
1.1.51	Os backups para Fita deverão ser gerados a partir de Backups já armazenados nos repositórios primários (Disco, NAS, Appliances de Backup).			
1.1.52	O software de proteção de dados deverá permitir a recuperação de backups de máquinas virtuais armazenados em fita diretamente na infraestrutura de Virtualização ou através da restauração em um repositório em disco para posterior restauração no ambiente de produção.			
1.1.53	Deverá ser possível delegar permissões de restauração para Administradores de Banco de Dados de modo que esses possam apenas restaurar itens da aplicação a qual a permissão lhes foi concedida através da console Web.			
1.1.54	O software de proteção de dados deverá oferecer meios para delegação de permissões a usuários de modo que estes possam efetuar restaurações de arquivo diretamente no local de origem, mesmo que não possuam permissão nos arquivos e diretórios e não possam ver o conteúdo do arquivo.			
1.1.55	O software de proteção de dados deverá suportar múltiplos jobs simultâneos de backup de Máquinas Virtuais.			
1.1.56	O software de proteção de dados não deverá necessitar de agentes para realizar Backups, Replicação e Recuperação de máquinas virtuais, produzindo backups de imagem da máquina virtual e operando a nível de bloco no hypervisor integrando nativamente com a API de Backup do Hypervisor.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.57	O software de proteção de dados deverá ser capaz de proteger uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.			
1.1.58	O software de proteção de dados deverá oferecer várias estratégias e opções de transporte de dados para tarefas de backup, tais como: Diretamente através da Rede de Área de Armazenamento (SAN). Diretamente do armazenamento por meio do Hypervisor I/O (Virtual Appliance). Através do uso da rede local (LAN). Diretamente do snapshot de storage. Diretamente do repositório NFS (Datastore NFS)			
1.1.59	O software de proteção de dados não deverá exigir licenças adicionais para o backup e recuperação granular assistida e consistente de máquinas virtuais das seguintes aplicações: - Microsoft Active Directory 2012R2 até 2022; - Microsoft SQL Server 2012R2 para Windows; - Oracle Database 11.G Release 2, 12C Release 1 e 2, 18c e 19c; - PostgreSQL 12 ou superior; - Tais aplicações deverão ser protegidas sem o uso de softwares externos ou de terceiros e o software deverá produzir backups do Tipo Application Consistent com ou sem plugins, agentes ou integrações proprietárias desenvolvidas especificamente para essas funções; - Deverá ainda permitir realizar a truncagem e transporte agendado de logs transacionais (transaction logs) para máquinas virtuais com SQL Server, PostgreSQL e Oracle.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.60	<p>O software de proteção de dados deverá permitir a integração com o Microsoft SQL Server rodando em máquinas virtuais, com ou sem a necessidade da instalação de agentes ou plugins, com as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Executar backup de bases de dados do SQL Server de forma “online”, ou seja, sem a parada do banco.</li><li>- Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 15(quinze) minutos.</li><li>- Permitir a montagem de uma base de dados SQL Server a partir dos arquivos de backup, sem necessidade de restauração completa da base para produção, permitindo executar procedimentos e visualizar dados através do SQL Server Management Studio ou ferramenta similar.</li><li>- Permitir recuperação granular de objetos de databases do SQL Server para o local original, ou para um servidor alternativo.</li><li>- Permitir recuperação de databases para o local original ou para um servidor alternativo.</li><li>- Permitir a recuperação instantânea da base de dados para o servidor de origem ou outro servidor com a mesma versão do SQL Server, permitindo ainda programar quando ocorrerá a ação de mudança (switchover) dos datafiles da recuperação instantânea para os datafiles definitivos ou possuir funcionalidade de replicação integrada com o banco de dados permitindo criar uma réplica secundária que permita o envio dos logs do servidor de produção para o servidor secundário com aplicação de agendamento automático. Será admitida a integração com snapshots do storage para garantir a consistência do banco de dados e possibilitar a recuperação instantânea.</li></ul>			
--------	---	--	--	--

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.61	<p>O software de proteção de dados deverá permitir a integração com o PostgreSQL rodando em máquinas virtuais, com ou sem a necessidade da instalação de agentes ou plugins, com as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Executar backup de bases de dados do PostgreSQL de forma “online”, ou seja, sem a parada do banco.</li><li>- Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 15 (quinze) minutos.</li><li>- Permitir a montagem de uma base de dados PostgreSQL a partir dos arquivos de backup, sem necessidade de restauração completa da base para produção, permitindo executar procedimentos e visualizar dados através do PGAdmin ou ferramenta similar.</li><li>- Permitir recuperação de databases para o local original ou para um servidor alternativo.</li><li>- Permitir a recuperação instantânea da base de dados para o servidor de origem ou outro servidor com a mesma versão do PostgreSQL, permitindo ainda programar quando ocorrerá a ação de mudança (switchover) dos datafiles da recuperação instantânea para os datafiles definitivos ou possuir funcionalidade de replicação integrada com o banco de dados permitindo criar uma réplica secundária que permita o envio dos logs do servidor de produção para o servidor secundário com aplicação de agendamento automático. Será admitida a integração com snapshots do storage para garantir a consistência do banco de dados e possibilitar a recuperação instantânea.</li></ul>			
--------	---	--	--	--

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.62	<p>O software de proteção de dados deverá permitir a integração com o Oracle rodando em máquinas virtuais, com ou sem a necessidade da instalação de agentes ou plugins, com as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Executar backup de bases de dados do Oracle de forma "online", ou seja, sem a parada do banco.</li><li>- Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 15 (quinze) minutos.</li><li>- Permitir a montagem de uma base de dados Oracle a partir dos arquivos de backup, sem necessidade de restauração completa da base para produção, permitindo executar procedimentos e visualizar dados através do Sqlplus ou possuir funcionalidade de replicação integrada com o banco de dados permitindo criar uma réplica secundária que permita o envio dos logs do servidor de produção para o servidor secundário com aplicação de agendamento automático.</li><li>- Permitir recuperação de databases para o local original ou para um servidor alternativo.</li></ul>			
1.1.63	<p>O software de proteção de dados deverá permitir a integração com Oracle Database, realizando o backup de forma "online" via Oracle RMAN através de plugin do Tipo SBT.</p>			
1.1.64	<p>O software de proteção de dados deve permitir a integração com SAP Hana, realizando backups de forma "online" via backint através do Hana Studio ou Cockpit, permitindo o controle de schedule pela ferramenta de backup;</p>			
1.1.65	<p>O software de proteção de dados permitir gerenciar de forma centralizada as políticas de backups via integração dos bancos de dados Oracle e Sap Hana, permitindo ao menos:</p> <ul style="list-style-type: none"><li>- Criar, editar e excluir Jobs de backup para Oracle RMAN e Hana Backint.;</li><li>- Configurar o backup de logs (archive logs);</li><li>- Possuir agendador próprio para o backup;</li><li>- Instalação remota e gerenciada dos plugins necessários para integração com o Oracle RMAN e SAP Hana Backint.</li><li>- Possuir mecanismo de recuperação a partir da console do software de proteção de dados de backup, sem a necessidade de usar scripts para efetuar restauração das bases de dados.</li></ul>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.66	<p>O software de proteção de dados deverá permitir a integração com Microsoft Active Directory rodando em máquinas virtuais, com ou sem a necessidade da instalação de agentes ou plugins, com as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Permitir a restauração granular a nível de objeto, por exemplo, objetos de usuário incluindo suas senhas.</li><li>- Permitir comparar os objetos com a produção, permitindo restaurar apenas os itens ausentes ou alterados.</li></ul>			
1.1.67	<p>O software de proteção de dados deve permitir a integração com DB2, realizando backups de forma “online” via IBM Db2 tools, através do IBM Db2 Call Level Interface, através do IBM Db2 Call Level Interface ou via agente de backup sem necessidade da utilização de scripts.</p>			
1.1.68	<p>O software de proteção de dados deverá estar licenciado e permitir integração com MySQL, executando o backup de bases de dados do MySQL de forma “online”, ou seja, sem a parada do banco e de forma consistente, ou via agente de backup sem necessidade da utilização de scripts.</p>			
1.1.69	<p>O software de proteção de dados deverá possuir recursos para ler e verificar a consistência do arquivo de backup no repositório. Em caso de detecção de blocos corrompidos o software de proteção de dados deverá automaticamente corrigir o arquivo copiando novamente aqueles blocos dos volumes de produção.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.70	<p>O software de proteção de dados deverá permitir a instanciação sob demanda de uma ou mais Máquinas Virtuais, que estejam salvas em backup, em ambiente virtual de laboratório com as seguintes características:</p> <ul style="list-style-type: none"><li>- Manter todas as configurações originais de rede das Máquinas Virtuais sem ocasionar nenhum conflito com o ambiente de produção, ou seja, deverá ser um ambiente de rede isolado.</li><li>- Permitir a comunicação de rede entre as Máquinas Virtuais dentro deste ambiente isolado.</li><li>- O software de proteção de dados deverá prover automaticamente uma Máquina Virtual com a função de proxy de rede, que permita a configuração de uma comunicação da rede isolada com o ambiente de rede de produção de uma forma segura.</li><li>- Prover meios automáticos para testar as aplicações e serviços rodando dentro de uma máquina virtual, de modo a garantir que não apenas o backup dela esteja íntegro, mas também o serviço e/ou a aplicação estão funcionais.</li><li>- O software de proteção de dados deverá ser capaz de inicializar, nesse ambiente isolado do ambiente de produção, uma ou um grupo de máquinas virtuais armazenadas no repositório de backup, possibilitando a resolução de problemas, realização testes de aplicação patches e testes de upgrades, tudo sem afetar os dados do ambiente de produção e sem modificar os backups. O processo deverá ser executado através de um assistente na interface gráfica da ferramenta de backup, sem a necessidade uso de scripts.</li></ul>			
1.1.71	<p>O software de proteção de dados deverá ser capaz de realizar testes automatizados de recuperabilidade automaticamente a partir das máquinas no repositório de backup, incluindo testes funcionamento dos serviços, como DNS, Active Directory, Rede, SQL Server, permitindo também a configuração de testes através do uso de scripts.</p>			
1.1.72	<p>O software de proteção de dados deverá fornecer uma estratégia de recuperação rápida, que permita aos usuários prover/restabelecer o serviço quase imediatamente e de maneira simples. Esta estratégia deve consistir em iniciar e ligar a máquina virtual, que falhou, diretamente do arquivo de backup no armazenamento usual do backup.</p>			



**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.73	A recuperação instantânea das máquinas virtuais deve permitir mais de uma máquina virtual e/ou ponto de restauração simultâneo para a disponibilidade do ponto de recuperação funcional, permitindo ter vários pontos no tempo de uma ou mais máquinas virtuais em execução.			
1.1.74	Após uma recuperação rápida, deve ser possível realizar uma restauração total sem interrupções de serviço. A ferramenta deverá garantir que o trabalho feito pelos usuários não seja afetado ao migrar suas máquinas virtuais do repositório de backup para o armazenamento de produção, sem impor uma restrição de tempo na execução da máquina durante o processo de recuperação instantânea.			
1.1.75	O software de proteção de dados deverá permitir a restauração do backup de Máquinas Virtuais VMWARE, criadas no ambiente on-premises, diretamente para instancias AWS EC2, Microsoft Azure e Google Compute Engine.			
1.1.76	O software de proteção de dados deverá permitir a restauração granular de arquivos e pastas de máquinas virtuais.			
1.1.77	<p>O software de proteção de dados deverá prover a capacidade de restauração de um, ou mais discos de uma máquina virtual, a partir dos repositórios de backup em disco, diretamente para o datastore de produção, configurando o disco diretamente na máquina virtual.</p> <ul style="list-style-type: none"><li>- Deverá ser possível restaurar o disco no formato original, como Thin ou Thick Provisioned.</li><li>- Deverá suportar a recuperação instantânea de discos de máquinas virtuais diretamente para o ambiente de produção, ou realizar a recuperação instantânea da máquina virtual completa para essa operação, possibilitando a montagem dos discos das máquinas virtuais, possibilitando a posterior migração para o datastore de produção.</li><li>- O software de proteção de dados também deve permitir a recuperação apenas dos blocos de disco da máquina virtual que foram alterados usando o CBT.</li></ul>			
1.1.78	O software de proteção de dados não deverá precisar de agentes para a recuperação granular de aplicações e arquivos dos sistemas suportados. Caso o software de proteção de dados necessite de agente para efetuar recuperação granular, será admitido desde que a instalação do agente seja feita de forma automatizada pelo software.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.79	Deverá haver uma opção de recuperação de arquivos que estão dentro dos backups das máquinas virtuais que deve permitir o acesso ao conteúdo dos discos virtuais dessas máquinas, sem a necessidade de recuperar o backup completo e reiniciar a máquina virtual a partir dele.			
1.1.80	O software de proteção de dados deverá incluir um assistente de recuperação instantânea em nível de arquivo nos sistemas de arquivos mais utilizados do Windows – FAT, FAT32, NTFS, ReFS. Linux – ext2, ext3, ext4, JFS, XFS, Btrfs.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.1.81	<p>O software de proteção de dados deverá ser capaz de realizar réplicas de máquinas virtuais em outros hosts, clusters, sites ou infraestruturas sem depender de replicação de Storage, com as seguintes características:</p> <ul style="list-style-type: none"><li>- A replicação deverá ocorrer em snapshots e checkpoints do hypervisor.</li><li>- Deverá permitir realizar a replicação a partir dos backups previamente realizados.</li><li>- Deverá utilizar as réplicas como fonte para recuperação de backups a nível de arquivo.</li><li>- Deverá permitir o Failover de uma máquina virtual para outro host ou cluster, bem como o Failback para o ambiente de origem através da console da ferramenta.</li><li>- Deverá apresentar um método de recuperação fácil para ambientes de contingência, com ações pré-configuradas para evitar ações manuais em caso de desastre.</li><li>- Deverá oferecer recursos para reconfiguração de endereços IPs das máquinas virtuais replicadas para outro site.</li><li>- Deverá ser capaz de replicar máquinas virtuais VMware entre diferentes cluster através de tecnologia de proteção de dados contínua (CDP), com RPO (Objetivos de Pontos de Recuperação) de 15 minutos ou inferior. Esse recurso deverá estar disponível para todo ambiente licenciado.</li><li>- O CDP deverá ser baseado em filtros de I/O do hypervisor, dispensando o uso de snapshots ou outros recursos externos para replicação (será permitida a utilização de ferramentas de terceiros para a funcionalidade de CDP, desde que o licenciamento destas ferramentas seja fornecido integralmente pela proponente e que a operação e monitoramento ocorram de forma integrada à interface principal da solução de backup).</li><li>- Deverá ser possível criar diferentes políticas de CDP, e deverá ser possível a realização de failover, failback e a criação de planos de failover das máquinas virtuais incluindo a reconfiguração de IP das máquinas virtuais.</li></ul>			
1.1.82	<p>O software de proteção de dados deverá ter a capacidade de relatar a conformidade com as políticas de proteção e disponibilidade de dados de acordo com os parâmetros definidos.</p>			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.1.83	O software de proteção de dados deverá permitir ações de correção para automatizar processos manuais rotineiros associados à solução de problemas comuns de infraestrutura virtual e de backup, como a eliminação de um snapshot de máquinas virtuais.			
1.1.84	O software de proteção de dados deverá incluir um VMware Plug-in para o vSphere Web Client e monitorar a infraestrutura de backup diretamente do vSphere Web Client, com exibições detalhadas e gerais do status das tarefas e dos recursos de backup.			
1.1.85	O software de proteção de dados deverá ser capaz de criar um índice (catálogo) de todos os arquivos gerenciados pelos sistemas operacionais Windows ou Linux, sem um agente, quando este for o sistema operacional executado dentro de uma máquina virtual cujo backup foi finalizado.			
1.1.86	Deverá ser possível realizar buscas de arquivos dentro dos backups, permitindo a procura pelo nome, tipo e tamanho, onde o software de proteção de dados deverá efetuar uma varredura em todos os backups indexados de diferentes máquinas virtuais e facilitar o processo de restauração.			
1.1.87	O software de proteção de dados ofertado deverá se enquadrar entre os líderes no relatório mais recente definido pelo Gartner, em seu quadrante mágico de "Data Center Backup and Recovery Solutions".			
1.2	Requisitos para Servidores Físicos			
1.2.1	Suportar a proteção completa de servidores físicos, workstations, desktops e notebooks com backups a nível de imagem, tanto em nível de arquivos, quanto em nível de volumes.			
1.2.2	Possuir agentes para no mínimo os seguintes sistemas operacionais: - Windows 10 ou superior - MacOS 11 ou superior - Windows Server 2012R2 ou superior - Red Hat Enterprise Linux 8 ou superior; - Suse Linux SLES 12/15; - Oracle Linux 7/8/9; - Ubuntu 16.04 ou superiores; - IBM AIX 7.1 ou superiores; - Oracle Solaris 10/11;			
1.2.3	Para agentes em servidores Windows deve suportar o backup através de snapshots de Storage (lan free).			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.2.4	Deve garantir a integridade sem uso de scripts das seguintes aplicações em servidores Windows: <ul style="list-style-type: none"><li>- Active Directory 2012R2 e superiores;</li><li>- Exchange Server standalone ou em DAG 2016 ou superior;</li><li>- Microsoft Sharepoint 2016 ou superior;</li><li>- SQL Server 2012 ou superior;</li><li>- Oracle standalone que não faça uso de ASM 11G Release2 ou superior;</li></ul>			
1.2.5	Deve garantir a integridade sem uso de scripts das seguintes aplicações em servidores Linux: <ul style="list-style-type: none"><li>- PostgreSQL 12 ou superior;</li><li>- MySQL 5.6 ou superior;</li><li>- Oracle standalone que não faça uso de ASM, na versão 11G Release2 ou superior;</li></ul>			
1.2.6	Deve permitir a cópia de logs de bancos de dados Oracle, PostgreSQL e SQL Server (logs transacionais com intervalo mínimo de 15 minutos).			
1.2.7	Permitir a criação de imagens de recuperação inicializáveis dos backups de Linux, UNIX e Windows para recuperação de desastres (funcionalidade conhecida como Bare-Metal Restore) de forma nativa e sem a utilização de software de terceiros.			
1.2.8	Suportar a recuperação de backups de sistemas operacionais Windows e Linux oriundos de máquinas físicas diretamente para um ambiente virtual VMware vSphere e Microsoft Hyper-V (P2V).			
1.2.9	Suportar a restauração do sistema inteiro para equipamentos com o mesmo hardware e para equipamentos com hardware diferente, com a opção de incluir drivers adicionais.			
1.2.10	Suportar a proteção de equipamentos com Microsoft Windows, suportando inclusive o backup e a recuperação do "system state" do Windows de forma nativa e sem a utilização de software de terceiros.			
1.2.11	Permitir a exclusão de diretórios e arquivos do backup.			
1.2.12	Permitir proteger automaticamente as unidades de armazenamento externas, tal como pen drives e HDs externos conectados, durante as rotinas de backup.			
1.2.13	Deve suportar a restauração granular das seguintes aplicações: <ul style="list-style-type: none"><li>- Active Directory;</li><li>- Exchange Server;</li><li>- SQL Server;</li><li>- Sharepoint Server;</li><li>- PostgreSQL;</li></ul>			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.3	Requisitos para Cargas de Trabalho em Nuvem:			
1.3.1	Deve permitir realizar backup de máquinas virtuais sem uso de agentes, utilizando as APIs nativas do hyperscale ao menos das seguintes plataformas: - Microsoft Azure – Virtual Machines - Amazon AWS – EC2 - Google Cloud Platform – Compute engine			
1.3.2	Deve suportar o envio de cópia dos backups para storage de objetos do próprio hyperscale.			
1.3.3	Em ambientes Azure e AWS deve suportar ativação de imutabilidade no storage de objetos para proteger as imagens de backup.			
1.3.4	Deve permitir criar camadas (tiers) de backup para armazenar os backups de longa retenção em camadas frias do storage de objeto, permitindo assim a otimização de custos com armazenamento.			
1.3.5	Deve permitir criar cópias do backup para fora do ambiente de origem; sendo necessário suportar o envio ao menos para storage de objeto de outro fabricante e armazenamento on-premises.			
1.3.6	Para ambientes Azure e AWS deve permitir realizar backups de aplicações de forma consistente através da integração com VSS ou de forma nativa, para máquinas virtuais Windows e o uso de pré-scripts para máquinas virtuais Linux.			
1.3.7	Deverá possuir no mínimo as seguintes opções restauração: - Restauração da máquina virtual completa a partir de um snapshot. - Restauração máquina virtual completa a partir de um backup armazenado em storage de objetos. - Restauração de um disco(volume) individual. - Restauração granular de arquivos, suportando ao menos os sistemas de arquivos: FAT, FAT32, NTFS, ext2, ext3, ext4, XFS. - Restaurar a máquina virtual completa para outro hyperscale suportado, realizando a conversão dela (v2v) de forma integrada sem a necessidade de executar scripts manuais.			
1.3.8	Realizar backup de banco de dados do Tipo PaaS (Platform as a Service), suportando no mínimo os seguintes SGDBs: Amazon: RDS (todas as variantes), DynamoDB; Google Cloud: PostgreSQL, MySQL; Azure: MS SQL Server;			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.3.9	Para ambiente Azure e AWS deve permitir realizar backup das configurações de rede (Virtual Network, VPC), sendo possível realizar a restauração das configurações de forma granular ou integrada.			
1.3.10	<p>Deve permitir realizar backup dados não estruturados armazenado de storage objetos (Amazon S3 object storage e Microsoft Azure blob storage). Com as seguintes características:</p> <ul style="list-style-type: none"> <li>- Os backups poderão ser armazenados em outro storage de objetos com object lock ativo ou em infraestrutura local desde que suporte e possua imutabilidade ativa;</li> <li>- Não serão aceitas soluções que façam uso de scripts para executar tal backup, a compatibilidade com backup de storage de objetos deve constar na documentação oficial do software de proteção de dados de backup.</li> <li>- Deve possibilitar restaurar os dados para o storage de objetos original ou para um novo bucket.</li> <li>- Deverá suportar restauração granular de dados para ele bucket ou para um novo local;</li> </ul>			
1.3.11	O software de proteção de dados deve ser integrado na mesma console de gerenciamento do ambiente on-premises, para permitir gerenciamento e visibilidade centralizada.			
1.4	Compatibilidade			
1.4.1	<p>O software de proteção de dados ofertado deverá oferecer suporte a máquinas virtuais (VMware) com no mínimo as seguintes características:</p> <p>Todos os tipos e versões de hardware virtual disponíveis nas versões suportadas do VMware.</p> <p>Todos os Sistemas Operacionais suportados pelo Fabricante VMware.</p>			
1.4.2	O software de proteção de dados deverá oferecer suporte e integração com O software de proteção de dados de Infraestrutura de Virtualização de Servidores VMware vSphere e ESXi nas versões 7.x ou superior.			
1.4.3	O software de proteção de dados deverá ainda oferecer suporte e integração com o vCenter Server nas versões 7.0 ou superior.			
1.4.4	O software de proteção de dados deverá oferecer suporte e integração com o VMware vCloud Director.			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.4.5	O software de proteção de dados deverá possuir integração com Microsoft Active Directory para autenticação da Console de Gerência.			
1.4.6	Compatibilidade com Windows Server Hyper-V nas versões 2016 ou superior, incluindo também o suporte para a versão Hyper-V Server (Free Hypervisor).			
1.4.7	Compatibilidade com Azure Stack HCI.			
1.4.8	Compatibilidade com o Microsoft System Center Virtual Machine Manager ou diretamente com o cluster Hyper-v, nas versões 2016 ou superior			
1.4.9	Compatibilidade com Nutanix AHV nas versões 6.8 e superiores.			
1.4.10	Compatibilidade com Oracle Linux Virtualization Manager 4.5.4 ou superior.			
1.4.11	Compatibilidade com Red Hat Virtualization 4.4 SP1 ou superior.			
1.5	Solução de Gerenciamento			
1.5.1	O software de proteção de dados deverá possuir console de gerenciamento gráfica com interface que permita a instalação em sistemas operacionais Windows. A console poderá ser instalada no servidor de backup e deverá ser possível a instalação e outros computadores para gerenciamento do servidor de backup, de modo que não seja necessário o uso do protocolo RDP para administração das tarefas de backup.			
1.5.2	O software de proteção de dados deverá incluir um console Web que forneça uma visão consolidada de implantações distribuídas e federação de vários servidores de backup, relatórios centralizados, alertas consolidados e restauração com autoatendimento de máquina virtual e no nível de sistema de arquivos (granular), com atribuição de permissões em máquinas virtuais individuais e aplicações, tal como SQL Server.			
1.5.3	O software de proteção de dados deverá ser capaz de enviar notificações por correio eletrônico (e-mail), traps SNMP com informações sobre o resultado da execução de suas tarefas.			
1.5.4	O software de proteção de dados deverá oferecer suporte a API Rest de modo que desenvolvedores possam consultar informações sobre objetos do ambiente de backup e executar operações básicas na ferramenta utilizando o protocolo HTTPS.			



**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.5.5	<p>O software de proteção de dados deverá permitir que as tarefas abaixo sejam realizadas pela interface gráfica central, sem a necessidade de scripts e sem a necessidade de acessar a interface do cliente:</p> <ul style="list-style-type: none"><li>- Permitir a instalação e aplicação de patches/upgrades de agentes remotamente;</li><li>- Permitir configurar backup de clientes de forma remota, ou seja, toda a configuração do backup que o cliente irá executar deve ser feita na própria console central, sem a necessidade de ter que configurar localmente o cliente.</li></ul>			
1.5.6	<p>O software de proteção de dados deverá armazenar de modo centralizado as informações de gerenciamento do software de backup incluindo:</p> <ul style="list-style-type: none"><li>- Objetos protegidos;</li><li>- Rotinas de backup e políticas de retenção;</li><li>- Arquivos e diretórios contidos nas fitas;</li><li>- Fitas e seu conteúdo;</li><li>- Fitas com cópias em cofres externos e demais informações de gerenciamento;</li></ul>			
1.5.7	<p>O software de proteção de dados deverá fornecer mecanismo de diagnóstico que analise os logs do software de proteção de dados para identificar proativamente e alertar sobre problemas de infraestrutura.</p>			
1.5.8	<p>O software de proteção de dados deverá ter uma base de conhecimento integrada nos alarmes, embora também deva apoiar a personalização dos alarmes e descrições da base de conhecimento.</p>			
1.5.9	<p>O software de proteção de dados deverá possuir extensão ou módulo para PowerShell ou Bash, de modo que seja possível realizar tarefas no servidor de backup através da linha de comando bem como a criação de scripts de automação.</p>			
1.5.10	<p>O software de proteção de dados deverá possuir recursos avançados de agendamento de rotinas de backup, para dias específicos, dias da semana recorrentes, dia do mês recorrente.</p>			
1.5.11	<p>O software de proteção de dados deverá permitir o encadeamento de jobs via interface gráfica, sem utilização de scripts que permita a uma rotina de backup sua execução apenas após o término da outra.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.5.12	O software de proteção de dados deverá permitir a criação e/ou atribuição de perfis aos usuários da ferramenta de backup de modo que seja possível atribuir ao menos os seguintes papéis: Operador de Backup, Operador de Restore, Operador de Fitas e Administrador do Backup.			
1.5.13	O software de proteção de dados deverá suportar a restauração de backup de forma remota, ou seja, na console central seleciona-se o backup, e para onde será realizada a restauração remota.			
1.5.14	O software de proteção de dados deverá possuir mecanismo de auditoria para o controle de acesso, em operações realizadas através de interface gráfica ou web e linha de comando (interface CLI), contendo no mínimo, as seguintes informações: data e hora da operação, usuário que realizou a operação, operação realizada.			
1.5.15	O software de proteção de dados deverá permitir a visualização em sua console gráfica ou geração de relatórios de backup, os quais permitam obter minimamente as seguintes informações: - Horário de início e término de uma rotina de backup; - Tempo de duração de uma rotina de backup; - Status do backup (situação): - Relação dos objetos incluídos na rotina de backup; - Horário de início e término do backup de cada objeto; - Tempo de duração do backup de cada objeto; - Volume de dados na origem durante a rotina de backup; - Volume de dados com compressão e deduplicação; - Taxa de deduplicação e compressão de dados;			
1.5.16	Suportar a geração de relatórios sobre o consumo de licenças;			
1.5.17	Permitir a retenção dos dados históricos por período mínimo de 12 meses.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.5.18	<p>A console web deverá oferecer relatórios operacionais básicos com no mínimo as seguintes informações:</p> <ul style="list-style-type: none"><li>- Estatísticas do Jobs – Nome do Job, Tipo, Plataforma, data e horário da última execução e status.</li><li>- Máquinas Virtuais e Jobs – Nome da Máquina Virtual, Nome do Job de Backup, quantidade de Pontos de Restauração, última e próxima execução.</li><li>- Relatório de Auditoria – Com informações realizadas pelos usuários, incluindo Nome do Usuário, Data e horário que o usuário realizou a operação, Tipo da operação.</li></ul>			
1.5.19	<p>O software de proteção de dados deverá oferecer um conjunto de relatórios capazes de apresentar informações do tipo:</p> <ul style="list-style-type: none"><li>- Relatórios que permitam planejamento de capacidade.</li><li>- Relatórios que permitam a determinação da ineficácia no uso de recursos.</li><li>- Relatórios que facilitem a visibilidade de tendências negativas e anomalias.</li><li>- Envio automático e programado de relatórios de auditoria para operações de recuperação e modificações em políticas de backup ou replicação.</li><li>- O software de proteção de dados deve conter relatórios para verificar se a infraestrutura virtual está pronta para executar backups e de acordo com boas práticas. Deve conter recomendações para a correção de um problema encontrado.</li><li>- O software de proteção de dados deve conter relatórios para a revisão após a implementação do software de proteção de dados de backup, para validar se ela está em conformidade com as boas práticas de implementação e configuração.</li></ul>			
1.5.20	<p>O software de proteção de dados deverá suportar a geração de relatórios de máquinas virtuais protegidas, contendo:</p> <ul style="list-style-type: none"><li>- Quantidade total de máquinas virtuais na infraestrutura virtual;</li><li>- Relação das máquinas virtuais, com quebra entre as que possuem backup e aquelas que não possuem backup;</li><li>- Quantidade de versões de backup armazenadas no backup para cada máquina virtual protegida;</li><li>- Data da última execução da rotina de backup com sucesso;</li><li>- Repositório no qual o backup do objeto está armazenado.</li></ul>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.5.21	<p>O software de proteção de dados deverá possuir relatórios padrões e customizáveis, disponíveis sem necessidade de alteração do código-fonte, uso de scripts ou customizações não oficiais, devendo estar disponíveis quando da implementação do software de proteção de dados, contendo minimamente as seguintes características:</p> <ul style="list-style-type: none"><li>- Permitir a segregação de acesso de acordo com o perfil do usuário, para monitorar a infraestrutura conectada;</li><li>- Permitir o envio automático e programado de relatórios por e-mail;</li><li>- Permitir inserir logomarca personalizada nos relatórios gerados;</li><li>- Permitir exportar os relatórios gerados nos formatos: Microsoft Excel e PDF ou em formato amigável, desde que de fácil interpretação e formatação adequada;</li><li>- Suportar a geração de relatórios de "charge-back" para o ambiente de backup;</li><li>- Suportar a geração e envio de alarmes automaticamente relacionados à infraestrutura virtual e do software de proteção de dados de backup;</li><li>- Relação sobre todos os objetos enviados para fitas, com informações sobre o Tipo de dado enviado, quantidade de versões de backup enviadas e em quais fitas estão localizados os dados;</li><li>- Relação sobre as fitas, com informações sobre os dados contidos nelas, espaço livre e utilizado;</li><li>- Relação sobre as fitas utilizados em backups de longa retenção do Tipo GFS(GrandfatherFather-Son) com informações sobre o período de retenção, quantidade de fitas em cada conjunto, as datas em que as cópias são criadas, e em quais fitas os dados estão localizados.</li></ul>			
--------	---	--	--	--

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.5.22	<p>O software de proteção de dados deverá conter relatórios avançados, tais como:</p> <ul style="list-style-type: none"><li>- Auditoria de alterações de objeto de backup;</li><li>- Auditoria de alterações da infraestrutura de backup;</li><li>- Modelagem em caso de falhas;</li><li>- Capacidade planejamento da infraestrutura backup;</li><li>- Crescimento de Máquinas;</li><li>- Capacidade planejamento de infraestrutura de backup;</li><li>- Avaliação de desempenho do armazenamento de dados do ambiente de backup;</li><li>- Avaliação de configuração da infraestrutura de backup;</li><li>- Estimativa da taxa de alteração dos objetos de backup;</li></ul>			
1.6	Recursos de Segurança			
1.6.1	<p>O software de proteção de dados ofertado deverá possuir mecanismos e funcionalidades de proteção (que deverão estar 100% licenciados) para atuar, e identificar sinais de ataques cibernéticos (Tipo “ransomware” – sequestro de dados), prevenindo a perda e/ou indisponibilidade de dados por remoção ou criptografia, considerando as seguintes características:</p>			
1.6.2	<p>Os dados armazenados nos repositórios de backup devem estar protegidos contra alterações indesejadas, e ser imutáveis, ou seja, não podem ser modificados por agentes externos ao backup, de modo que eles só possam ser alterados ou removidos mediante expiração do backup e respeitar o período estabelecido para remoção;</p>			
1.6.3	<p>Possuir mecanismos que impeçam a deleção de backups do armazenamento do backup (funcionalidades do Tipo “Ransomware Protection”) que garantam a imutabilidade dos backups no armazenamento de backup.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.6.4	<p>O software de backup deve possuir o recurso de dupla aprovação (Four Eyes Principle) para executar atividades administrativas de exclusão no equipamento, sendo necessário exigir a autenticação e autorização de um segundo usuário (escalação) para concluir a alteração dos seguintes parâmetros críticos:</p> <ul style="list-style-type: none"><li>- Deleção de uma imagem de backup;</li><li>- Adição, edição e remoção de administradores de backup;</li><li>- Ativação e desativação de MFA (multifator authentication);</li><li>- Resetar o uso de MFA para um usuário específico.</li><li>- Remoção de repositórios de backup e storages da infraestrutura de backup.</li><li>- Será admitido a customização de tarefas que viabilizem a dupla aprovação.</li></ul>			
1.6.5	<p>O software de backup deve possuir mecanismo de duplo fator de autenticação (MFA), com suporte a autenticação com o protocolo OpenID ou SAML.</p>			
1.6.6	<p>O software de backup deve suportar e estar licenciado com a funcionalidade de criptografia do Tipo DARE (Data At Rest Encryption) de no mínimo 256 bits com certificação FIPS 140-2.</p>			
1.6.7	<p>Deve possuir integração com sistemas de KMS (Key Management System) do tipo assimétrico, permitindo assim que a chaves de criptografias associadas aos backups sejam rotacionadas.</p>			
1.6.8	<p>Deve suportar criptografia em trânsito (in Flight) visando proteger o conteúdo do backup durante o transporte dos dados;</p>			
1.6.9	<p>O software de proteção de dados deve prover recursos de validação dos dados armazenados nos repositórios de backup para verificar e garantir a integridade deles;</p>			
1.6.10	<p>O software de proteção de dados deve utilizar métodos de análise Física de validação dos dados como: verificação de redundância cíclica (CRC), que realiza validação dos dados a nível de blocos, permitindo a identificação de blocos corrompidos e ações de correção:</p> <p>A rotina de validação dos dados deve permitir o agendamento e ser executada periodicamente para garantir a integridade dos dados armazenados;</p> <p>No caso de identificação de blocos corrompidos, O software de proteção de dados deve enviar alertas e notificações aos responsáveis;</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.6.11	A solução deve possuir mecanismos de detecção de malware em tempo de execução (inline detection), sendo que este mecanismo deve ser capaz de detectar possíveis sinais de criptografia e artefatos de texto criados pelo malware, em caso de ocorrência deste tipo de comportamento a solução de backup deve marcar o ponto de recuperação como suspeito. Alternativamente serão aceitas soluções que provem monitoramento, detecção e remediação de Ameaças (Threat Monitoring, Detection and Remediation), provendo visibilidade, correção de anomalias e falhas de backup.			
1.6.12	Possuir mecanismo de detecção de malware através da análise e indexação de conteúdo visando identificar: Arquivos e extensões conhecidas de arquivos de malware. Detecção de arquivos renomeados em massa. Deleção de arquivos em massa.			
1.6.13	Deve possuir integração com ferramentas de cyber segurança para identificar assinaturas de malware dentro das imagens de backup, sendo compatível com YARA ou ferramenta similar para identificar anomalias de maneira online. Além disso, deve fazer uso de inteligência artificial para monitoramento, detecção e, se possível, remediação de ameaças e anomalias no backup e restauração dos dados.			
1.6.14	Deve possuir integração via API com ferramentas de cyber segurança do Tipo MDR (Managed Detection and Response), permitindo que o software de proteção de dados de MDR envie informações sobre malwares que possam estar infectando máquinas virtuais ou servidores Físicos, suportando no mínimo as seguintes integrações: Gerar notificação de suspeitas/objetos infectados ou marcar as imagens de backup associadas ao objeto como suspeitas /infectadas ; Deve permitir a execução automática de um backup após o recebimento da notificação;			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.6.15	Monitoramento Ativo: Quando alterações anômalas forem detectadas, alertas deverão ser acionados. O software de proteção de dados deverá possuir mecanismos que permitam que alertas sejam integrados a informações de segurança e gerenciamento de eventos (SIEM), outros sistemas de resposta a incidentes ou iniciar fluxos de trabalho.			
1.6.16	O software de proteção de dados deve permitir a criação de uma estratégia de segurança que permita a utilização de armadilhas para atrair e desviar cyber criminosos, gerando alertas antecipados e reduzindo os danos causados as cópias de segurança realizadas. Alternativamente serão aceitas soluções que possuam mecanismos de monitoramento proativo e persistente do servidor de backup, que permita identificar possíveis ameaças analisando no mínimo logs, comunicação de rede e processos/serviços do servidor de backup e possuir detecção de táticas, técnicas e procedimentos (TTPs) que caracterizam a execução de ransomware. Esses TTPs devem ser coletados e mapeados para o framework do MITRE ATT&CK.			
1.7	Recursos de Disaster Recovery (DR).			
1.7.1	O software de proteção de dados ofertado deverá possuir mecanismos e funcionalidades de orquestração de desastres (que deverão estar 100% licenciados), permitindo a recuperação completa de máquinas virtuais VMware e servidores Físicos Windows e Linux de forma automatizada, suportando ao mínimo os seguintes Tipos de recuperação: - Failover de máquinas virtuais replicadas para outro site VMware. - Recuperação de máquinas virtuais, a partir de imagens de backup para outro site VMware. - Recuperação de máquinas virtuais, a partir de imagens de backup para o Microsoft Azure (IaaS) ou Amazon AWS EC2.			
1.7.2	Deve permitir armazenar credencias de forma criptografada em uma base central, para uso posterior dentro dos planos de recuperação.			



**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.3	<p>Deve permitir categorizar a infraestrutura e criar locais de recuperação pré-definidos incluindo ao menos as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Definição de recursos computacionais para a recuperação (Clusters ou Hosts).</li><li>- Definição de recursos de armazenamento para a recuperação, deve permitir ainda limitar a capacidade máxima de uso do storage durante o processo de recuperação. Será admitido que o ajuste e limitação da capacidade seja efetuada pelo sistema de armazenamento.</li><li>- Deve permitir remapear a rede das máquinas virtuais (Port Groups) do site de origem para o site de destino, caso o site de destino use outra infraestrutura de rede.</li><li>- Deve permitir remapear a rede dos servidores Físicos, usando regras de descoberta baseadas no endereçamento IP de origem e executar o remapeamento para o port group da infraestrutura virtual de destino.</li><li>- Deve permitir executar regras de Re-IP para servidores e máquinas virtuais Windows. Para VMs Linux será aceito o uso de scripts.</li></ul>			
1.7.4	<p>Em caso de DR para Cloud deve permitir categorizar a infraestrutura e criar locais de recuperação pré-definidos incluindo ao menos as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>- Definir a subscrição (account) onde as máquinas virtuais serão criadas, incluindo a possibilidade de escolher uma região específica.</li><li>- Permitir selecionar de qual repositório os backups serão restaurados.</li><li>- Definir o Resource Group onde as máquinas virtuais serão criadas.</li><li>- Permitir realizar o mapeamento da Virtual Network (VPC), Subnet e NSG.</li><li>- Permitir criar regras de mapeamento para modelos de máquina virtual da cloud para uso nos planos de recuperação ou selecionar automaticamente o modelo conforme previamente criado.</li><li>- Permitir elencar uma rede de quarentena para uso em casos em que as imagens de backup possam estar infectadas.</li></ul>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.5	<p>Deve possuir ações pré-definidas de testes que possam ser executadas em determinada fase do plano ou até mesmo diretamente a uma máquina virtual ou servidor, suportando no mínimo as seguintes ações:</p> <ul style="list-style-type: none"><li>- Ligar e desligar uma máquina virtual.</li><li>- Efetuar a checagem de “heartbeat” na máquina virtual.</li><li>- Executar um teste de ping contra a máquina virtual/servidor que está sendo processada.</li><li>- Iniciar um serviço na máquina virtual/servidor que está sendo processada.</li><li>- Verificar a conectividade com aplicações através de testes de conectividade na porta da aplicação, suportando de forma pré-definida ao menos (DNS, Domain Controller, Mail Server, Domain Global Catalog, Web Server).</li><li>- Deve permitir executar ações associadas aos Jobs de backup e replicação, permitindo que durante a execução de um plano de restauração ou failover seja possível ao menos (iniciar e parar, desativar ou ativar) um ou mais Jobs especificados.</li><li>- Deve permitir testar a conectividade com Websites do IIS e Sharepoint.</li><li>- Deve permitir testar a conectividade com bancos de dados SQL a nível de instancia e database.</li><li>- Deve permitir enviar notificações por e-mail durante a execução do plano.</li><li>- Deve permitir criar scripts customizados para cobrir itens adicionais aos já citados aqui com ao menos as seguintes características:</li><li>- Ser possível passar informações através de parâmetros para dentro do script, tais como (credenciais, nome da máquina virtual, endereço IP, valor customizado).</li><li>- Toda a saída (output) do script deve ser listada na console e nos relatórios de testes e execução dos planos associados.</li></ul>			
-------	--	--	--	--

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.6	<p>Caso a solução não execute da maneira descrita no item 1.7.5, deve executar no mínimo as seguintes funções:</p> <p>a) Deve possuir capacidade de executar as seguintes operações para as máquinas virtuais pertencentes ao plano de replicação:</p> <ul style="list-style-type: none"><li>- Testar inicialização da VM:</li><li>- Ligar as VMs de destino para verificar se elas estão prontas para uso em caso de desastre. Para evitar conflitos com a VM de origem deve garantir que a máquina virtual não seja modificada pelo teste de inicialização, este cenário devera tirar um snapshot da máquina virtual antes do teste de inicialização, inicializar as VMs de destino com as conexões de rede desativadas e reverter para o snapshot posteriormente.</li><li>- Testar Failover: Executar uma operação de teste de failover para um site de destino de teste para um par de replicação ou grupo de VMs.</li><li>- Replicação reversa: Atualizar a VM de origem no site primário com as alterações da VM em execução no site secundário.</li><li>- Failover de ponto no tempo: Selecionar um ponto de recuperação no tempo para usar na operação de failover.</li><li>- Failover planejado: Executar um failover planejado para que você possa testar o processo de failover ou executar manutenção em seu site primário.</li><li>- Failback: Retornar ao site primário após um failover.</li><li>- Failover não planejado: Caso o site primário não esteja disponível, deverá desativar a replicação e ligar as VMs de destino no site de recuperação de desastres com conexões de rede e endereços IP apropriados.</li></ul> <p>b) Deve possuir ferramenta própria do fabricante da solução para realizar o planejamento do plano de replicação e cálculo do RPO e RTO apropriados para o plano em questão, provendo assim documentação das capacidades customizadas para o ambiente.</p>			
1.7.7	<p>Deve possuir mecanismos que permitam realizar simulações completas do plano de recuperação em ambiente isolado (sandbox), testes estes que podem ser feitos através de recuperação instantânea (sem consumir espaço em disco no storage produtivo) ou até mesmo testes de restore completos a fim de validar o tempo de RTO do plano em questão.</p>			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
1.7.8	Deverá ser possível agendar a execução dos testes em um calendário programável.			
1.7.9	O software de proteção de dados de suporta a criação de múltiplos planos de recuperação/failover.			
1.7.10	O software de proteção de dados deve possuir mecanismos de RBAC como no mínimo os seguintes Tipos de papéis: - Administrador completo do software de proteção de dados. - Autor e Operador de planos.			
1.7.11	O software de proteção de dados deve permitir a criação de escopos de trabalho e através destes escopos limitar o acesso dos usuários ao menos os seguintes tipos de objetos: - Grupos, incluindo (VMs, Hosts, Storage, Clusters, Jobs de backup) - Locais de recuperação. - Ações pré-definidas. - Credências armazenadas no software de proteção de dados.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.12

Deverá permitir a criação e execução de planos de recuperação ou failover com no mínimo as seguintes funcionalidades:

- Deverá permitir a definição dos valores desejados de RPO (Recovery Point Objective) e RTO (Recovery Time Objective) para o plano em questão.
- Deverá permitir a execução de rotinas de validação, e avaliar o RTO real do plano em um cenário de desastres, alertando em caso de não atendimento ao SLA definido como objetivo.
- Definir para qual local será efetuado o restore ou failover.
- Executar scan de antivírus nos discos da máquina virtual ou servidor.
- Executar varredura nos discos da máquina virtual ou servidor visando encontrar assinaturas de malwares através de ferramentas como Yara ou similares.
- Permitir criar grupos de máquinas virtuais que serão processadas pelo plano de recuperação sendo que cada grupo deve incluir ao mínimo as seguintes funcionalidades:
  - a) Mecanismo de descoberta das VMs através de Tags e queries customizados associadas a infraestrutura de virtualização.
  - b) Definição do método de execução de forma sequencial ou paralela, de forma paralela deve ainda permitir limitar a quantidade máxima de VMs ou agentes.
  - c) Definir quais ações predefinidas serão executadas nas máquinas virtuais ou servidores Físicos.
  - d) Deverá possibilitar definir ações pré-definidas de forma individual para cada máquina virtual ou servidor.

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.13	<p>Caso a solução não execute da maneira descrita no item 1.7.12, deve executar no mínimo as seguintes funções:</p> <p>a) Deve possuir capacidade de executar as seguintes operações para as máquinas virtuais pertencentes ao plano de replicação:</p> <ul style="list-style-type: none"><li>- Testar inicialização da VM: Ligar as VMs de destino para verificar se elas estão prontas para uso em caso de desastre. Para evitar conflitos com a VM de origem deve garantir que a máquina virtual não seja modificada pelo teste de inicialização, este cenário devera tirar um snapshot da máquina virtual antes do teste de inicialização, inicializar as VMs de destino com as conexões de rede desativadas e reverter para o snapshot posteriormente.</li><li>- Testar Failover: Executar uma operação de teste de failover para um site de destino de teste para um par de replicação ou grupo de VMs.</li><li>- Replicação reversa: Atualizar a VM de origem no site primário com as alterações da VM em execução no site secundário.</li><li>- Failover de ponto no tempo: Selecionar um ponto de recuperação no tempo para usar na operação de failover.</li><li>- Failover planejado: Executar um failover planejado para que você possa testar o processo de failover ou executar manutenção em seu site primário.</li><li>- Failback: Retornar ao site primário após um failover.</li><li>- Failover não planejado: Caso o site primário não esteja disponível, deverá desativar a replicação e ligar as VMs de destino no site de recuperação de desastres com conexões de rede e endereços IP apropriados.</li></ul> <p>b) Deve possuir ferramenta própria do fabricante da solução para realizar o planejamento do plano de replicação e cálculo do RPO e RTO apropriados para o plano em questão, provendo assim documentação das capacidades customizadas para o ambiente.</p>			
--------	--	--	--	--

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

1.7.14	<p>Deverá possuir relatórios padrões e customizáveis, permitindo:</p> <ul style="list-style-type: none"><li>- Criar relatórios automáticos de conformidade baseado nos planos e testes de recuperação de desastre.</li><li>- Adicionar logomarca aos relatórios e personalizar totalmente a documentação, com baseado em modelos editáveis.</li><li>- Gerar automaticamente relatórios para documentar todas as etapas do plano de recuperação de desastres.</li><li>- Gerar automaticamente relatórios de execução das operações de restore e failover.</li><li>- Gerar automaticamente relatórios de execução das operações de teste dos planos de restore e failover.</li><li>- Gerar documentação com base em modelos, capaz de documentar todas as etapas e processos necessários para recuperação em caso de desastre.</li><li>- Validar se o plano corresponde à configuração atual do ambiente e se estão prontos para funcionar com verificações de disponibilidade do plano a serem completadas.</li></ul>			
2	<b>SOLUÇÃO PARA PROTEÇÃO DE AMBIENTE KUBERNETES /TANZU</b>			
2.1	O software de proteção de dados ofertado deverá possuir softwares pertencentes ao mesmo fabricante, não sendo aceitas composições de softwares de fabricantes distintos para o atendimento as especificações.			
2.2	O software de proteção de dados ofertado não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante.			
2.3	Caso o licenciamento do software de proteção de dados para ambiente Kubernetes/Tanzu seja licenciado pelo número de nós, não deverá possuir nenhum tipo de restrição de limite de volumetria de armazenamento (TB), seja por Back-End ou Frontend, em quaisquer componentes do software de proteção de dados durante a vigência do CONTRATO. Já se o licenciamento do software de proteção de dados para ambiente Kubernetes/Tanzu seja licenciado pelo volume de Frontend, não deverá haver limites quanto ao número de worknodes protegidos.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

2.4	O licenciamento deverá prover proteção para 50 (cinquenta) nós (worker nodes) quer sejam máquinas físicas ou virtuais, ou uma volumetria líquida de no mínimo de 700 (setecentos) TB (Terabytes) de frontend.			
2.5	Prover licenciamento contabilizando apenas o número de nós (worker nodes) ou volumetria de frontend que compõe o software de proteção de dados, independentemente de suas configurações de hardware (vCPUs, memória, discos e dentre outras), da localização lógica ou geográfica do hospedeiro em que estiver sendo executada, suportando ambientes on-premises e em nuvens públicas, conforme descrito na especificação deste Termo de Referência.			
2.6	Prover licenciamento de software baseado em assinatura ou subscrição, devendo todas as funcionalidades solicitadas neste documento estarem operacional e disponíveis durante toda a vigência do CONTRATO. Não poderão ser cobrados quaisquer valores adicionais para a recuperação dos dados já protegidos durante e após o término do CONTRATO.			
2.7	O software de proteção de dados ofertado deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do Fabricante, ou com end-of-life ou end-of-support anunciado.			
2.8	Prover licenciamento que englobe todas as funcionalidades e requisitos elencados neste Termo de Referência, sem nenhum tipo de cobrança adicional para a CONTRATANTE.			
2.9	O sistema de backup deve conseguir acesso ao cluster Kubernetes através do suporte a pelo menos um destes tipos de autenticação: <ul style="list-style-type: none"><li>- Certificados de cliente X509</li><li>- Bootstrap tokens do Kubernetes</li><li>- Service account tokens do Kubernetes</li><li>- Kubeconfig file</li></ul>			
2.10	O software de proteção de dados ofertado deverá possuir compatibilidade conforme as especificações abaixo:			



**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

2.10.1	Deve possuir integração com API nativa do Kubernetes, comportando políticas de backup no nível dos objetos desta plataforma, como Namespaces, Deployments, StatefulSets, PersistentVolumes, ou qualquer CustomResourceDefinition definido no ambiente, não sendo aceitos scripts ou backups no nível de sistema de arquivos para atendimento a esse item.			
2.10.2	Deve suportar diferentes distribuições de Kubernetes, incluindo distribuições compatíveis com a Cloud Native Computing Foundation (CNCF) e demais alternativas do mercado, como Rancher, Red Hat OpenShift e Vmware Tanzu;			
2.10.3	Deve suportar distribuições de Kubernetes em nuvens públicas, incluindo Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) e Google Kubernetes Engine (GKE).			
2.10.4	Deve permitir o backup e restore como frontend e backend de compartilhamentos de rede NAS (CIFS e NFS) e em Object Storage compatível com S3;			
2.10.5	Deve suportar compressão e deduplicação dos dados protegidos.			
2.10.6	Deve suportar a proteção de dados persistentes contidos em volumes de armazenamento (PersistentVolumes/PersistentVolumeClaims) através da especificação da Container Storage Interface (CSI), sendo, portanto, compatível com drivers que implementam esta especificação.			
2.10.7	Deve realizar o backup completo do Namespace e seus objetos como: Pods, Secrets, Deployments, Replica set, Certificates, ConfigMaps e Persistent Volumes.			
2.10.8	Deve ser possível a visualização dos diversos clusters Kubernetes e seus componentes protegidos a partir da console de gerenciamento de backup.			
2.10.9	Deve ser capaz de realizar a descoberta automática de namespaces dentro de um cluster.			
2.10.10	Deve realizar a descoberta automática dos containers e seus volumes persistentes configurados.			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

2.10.11	Deve suportar regras dinâmicas para filtrar/selecionar quais recursos do Kubernetes serão protegidos através de tipos específicos, nomes específicos ou pelos marcadores (labels) definidos em cada objeto. Da mesma forma, também deve ser possível filtrar/selecionar quais PersistentVolumes terão seus dados persistidos protegidos pela solução de backup.			
2.10.12	Possuir políticas de backup com agendamento automático do backup, permitindo escolher a frequência do backup e suas retenções.			
2.11	Deve permitir a restauração dos objetos protegidos em seu estado originalmente observado ou, quando estes forem delimitados a um Namespace do Kubernetes, suportar a restauração: - Para o Namespace original, pré-existente ou não; - Para um Namespace diferente do original, pré-existente ou não Restore para um novo Namespace;			
2.12	Deve permitir excluir determinados volumes persistentes (PV) durante a rotina de backup.			
2.13	Possuir interface gráfica para configuração e gerenciamento da proteção de ambiente Kubernetes.			
2.14	Deve suportar armazenamento imutável dos backups armazenados em Object Storage compatível com S3;			
2.15	Deve ser capaz de prover consistência das aplicações durante o backup, podendo capturar os objetos de aplicação e suas respectivas dependências;			
2.16	Deve prover proteção com consistência das aplicações (application consistent), de base de dados (database consistent) e opção de backups sem consistência (crash consistent);			
2.17	Deve suportar criptografia dos dados protegidos, usando o algoritmo AES-256;			
2.18	Deve permitir restaurações e migrações de aplicações nos seguintes formatos:			
2.18.1	Cross-Namespase: A aplicação pode ser migrada entre namespaces diferentes no mesmo cluster;			
2.18.2	Cross-Cluster: A aplicação é migrada entre clusters Kubernetes não federados;			
2.18.3	Cross-Account: Mobilidade pode adicionalmente ser feita entre clusters rodando em contas diferentes (Exemplo contas AWS) ou projetos (exemplo, Google Cloud projects);			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
2.18.4	Cross-Region: Mobilidade pode ser adicionalmente executada entre diferentes regiões do mesmo provedor de nuvem (exemplo, da US-East para a US-West).			
2.18.5	Cross-Cloud: A mobilidade pode ser feita entre diferentes provedores de nuvem (exemplo da AWS para Azure).			
2.19	Deve permitir modificação de recursos Kubernetes durante o processo de recuperação. Essas modificações podem ser usadas em um modelo granular para uma simples substituição de um Secret ou outro objeto, ou para permitir migração entre distribuições diferentes. Deve permitir testar se a modificação irá funcionar antes de iniciar o processo de restauração;			
2.20	Deve suportar autenticação OIDC (OpenID Connect) ou baseada em Token;			
2.21	Deve suportar instalação em ambientes Kubernetes isolados (Air-Gapped) sem conexão com a internet;			
2.22	Deve suportar RBAC (Role Based Access Control), permitindo criação de perfis de usuários diferentes para cada Tipo de atuação necessária na ferramenta;			
2.23	Deve suportar instalação dos componentes em um cluster Kubernetes, sem requerer a utilização de DaemonSets para seu funcionamento;			
2.24	Deve suportar execução das rotinas de proteção em paralelo.			
3	SOLUÇÃO DE PROTEÇÃO PARA MICROSOFT 365			
3.1	O software de proteção de dados ofertado deverá possuir softwares pertencentes ao mesmo fabricante, não sendo aceitas composições de softwares de fabricantes distintos a o atendimento as especificações.			
3.2	O software de proteção de dados ofertado não pode ser do Tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante.			
3.3	Sobre o Licenciamento:			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

3.3.1	Prover licenciamento do Tipo subscrição de direito de uso de software pelo período de 60 meses, por usuário do Microsoft 365. Ao término do período de subscrição, o software deverá permanecer totalmente operacional para as funcionalidades de restore/recovery (recuperação de dados já copiados/protegidos), sem a necessidade de pagamento de quaisquer valores adicionais pelo seu uso para a restauração de cópias de segurança realizadas durante a vigência da subscrição.			
3.3.2	Prover suporte técnico do fabricante e direito de atualização do software de proteção de dados pelo mesmo período de 60 (sessenta) meses de subscrição.			
3.3.3	Prover licenciamento para 16.000 usuários sem nenhum tipo de limite por volumetria, seja de backend ou frontend, em qualquer componente do software de proteção de dados durante a vigência da subscrição.			
3.3.4	Prover licenciamento que englobe todas as funcionalidades e requisitos elencados neste anexo e item, independentemente de qualquer quantidade de utilização do referido serviço, sem nenhum Tipo de cobrança adicional para a CONTRATANTE.			
3.3.5	O licenciamento deverá ser capaz de fazer backup e recuperar dados no Microsoft 365, com base em um licenciamento por usuário.			
3.3.6	Prover licenciamento de software baseado em subscrição, devendo todas as funcionalidades solicitadas neste documento estarem operacionais e disponíveis durante toda a vigência da subscrição. Não poderão ser cobrados quaisquer valores adicionais para a recuperação dos dados já protegidos durante e após o término da vigência da subscrição.			
3.3.7	O software de proteção de dados ofertado deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do Fabricante.			
3.4	Sobre a Integração:			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

3.4.1	<p>Deve possuir integração com Microsoft 365, suportando minimamente a proteção dos seguintes itens:</p> <p>EXCHANGE ONLINE:</p> <ul style="list-style-type: none"><li>a) Calendário;</li><li>b) Tarefas;</li><li>c) E-mail;</li><li>d) Contatos;</li><li>e) Caixas de e-mail compartilhadas</li></ul> <p>ONEDRIVE:</p> <ul style="list-style-type: none"><li>a) Pastas;</li><li>b) Arquivos individuais;</li></ul> <p>EQUIPE DO TEAMS:</p> <ul style="list-style-type: none"><li>a) Arquivos;</li><li>b) Posts;</li><li>c) Chats;</li><li>d) Equipes;</li></ul> <p>SHAREPOINT ONLINE:</p> <ul style="list-style-type: none"><li>a) Site inteiro;</li><li>b) Arquivos individuais.</li></ul>			
3.5	Sobre as Funcionalidades:			
3.5.1	<p>Operação de recuperação dos dados, no mínimo, nos seguintes níveis:</p> <ul style="list-style-type: none"><li>- MICROSOFT EXCHANGE: caixa postal completa e itens individuais (arquivos, e-mail, contatos, calendário);</li><li>- ONEDRIVE: pasta completa e arquivos individuais;</li><li>- TEAMS: conversas, posts e arquivos;</li><li>- SHAREPOINT: site completo e arquivos individuais;</li></ul>			
3.5.2	<p>Para operação de recuperação de versões anteriores deverá disponibilizar, no mínimo, as seguintes formas de recuperação dos dados:</p> <ul style="list-style-type: none"><li>- Recuperação para o local de origem;</li><li>- Fazer download do arquivo;</li></ul>			
3.5.3	<p>Deverá permitir enviar notificações sobre os resultados das tarefas de backup por e-mail ou disponibilizadas em uma central de notificações.</p>			
3.5.4	<p>O software de proteção de dados deve criptografar a comunicação entre o Microsoft 365 e a infraestrutura de backup usando SSL.</p>			
3.5.5	<p>Deve possuir mecanismo que permita comparar o conteúdo de uma caixa postal armazenada em backup com a versão produtiva, simplificando assim as operações de recuperação granular ou permitir a recuperação do mesmo em local diferente ao de produção para operação da restauração de itens.</p>			

**ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS**

3.5.6	Deve possuir formas para evitar throttling durante as operações de backup, suportando a adição de contas de serviço auxiliares ou de múltiplos Azure Apps;			
3.5.7	Deverá oferecer a capacidade de ajuste do uso da largura de banda durante as tarefas de backup;			
3.5.8	O software de proteção de dados deve ter a opção de executar a criptografia AES de 256 bits dos dados gravados em Object Storage compatível com S3.			
3.5.9	A implementação deve permitir a configuração ou geração de políticas de retenção.			
3.5.10	Deverá suportar o armazenamento dos dados localmente, seja em volumes locais ou apresentados via SAN, além de suportar o armazenamento em ambiente Cloud gravando em Object Storage compatível com S3.			
3.5.11	O software de proteção de dados deverá criar várias tarefas de backup na mesma organização do Microsoft 365, permitindo a inclusão ou exclusão de tipos de objetos de acordo com as necessidades da organização. Para tarefas de backup configuradas, deve ser possível configurar a seguinte opção de agendamento: Execução diária em horários e dias específicos;			
3.5.12	O software de proteção de dados deverá fornecer uma interface para exibir as estáticas dos objetos processados em cada sessão de backup.			
3.5.13	O software de proteção de dados deverá ter a capacidade de procurar itens do Exchange a partir de uma interface guiada sem a necessidade de processos de recuperação anteriores.			
3.5.14	O software de proteção de dados deve ter a capacidade de recuperar uma caixa de correio inteira ou selecionar individualmente quaisquer itens e recuperá-los para qualquer caixa de correio existente, ou exportá-los para arquivos .PST ou .EML.			
3.5.15	Oferecer suporte ao mecanismo de autenticação moderna (Modern authentication) para operações de backup e suporte a autenticação multifator (MFA) para processos de restauração ou para acesso a console centralizada.			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
3.5.16	O software de proteção de dados deve oferecer opções de retenção com base na data de criação dos itens em seu local original, ou baseadas na data de execução dos backups.			
3.5.17	Permitir exportar o conteúdo de backup, possibilitando o armazenamento dos dados em repositórios externos do software de proteção de dados.			
3.5.18	Deve possuir portal de autosserviço que permita os usuários finais executem seus próprios processos de restauração de dados através de uma interface familiar.			
3.5.19	Não deve depender da criação de usuários locais para dar acesso ao portal de autosserviço e deve suportar sso (Single sign-on) através das credências do próprio tenant de Microsoft 365.			
3.5.20	Deve possuir mecanismos que permitam limitar quais caixas postais, sites e equipes do Teams podem ser associadas a um usuário com permissões de restauração.			
3.5.21	Deve possuir mecanismo de Rest API.			
3.6	Sobre Relatório e Monitoramento:			
3.6.1	Disponibilizar logs de auditoria para as operações dos usuários realizadas na plataforma com, no mínimo, as seguintes informações: - Arquivos baixados (download); - Arquivos recuperados;			
3.6.2	Deve incluir relatórios para identificar estado da proteção de caixas de correio do Microsoft 365, gerenciar o uso de licenças e obter visibilidade sobre o consumo de armazenamento.			
3.6.3	O software de proteção de dados deve disponibilizar ferramenta de monitoramento dos backups e componentes do software de proteção de dados de backup para Microsoft 365 e se possível integrar com o software de proteção de dados de backup de VMs para visualização centralizada.			
4	PROTEÇÃO DE WORKLOADS			
4.1	A solução deverá realizar backup de banco PostgreSQL 9 ou superior.			
4.2	A solução deverá realizar backup de banco SQL Server 2019 ou superior.			
4.3	A solução deverá realizar backup de banco MySQL 8.0 ou superior.			
4.4	A solução deverá realizar backup de banco Sybase 15.6 ou superior, será aceito uso de scripts para execução do backup desde que integrados diretamente na política de backup através do conceito de pré/pós script.			

ITEM 1 - REQUISITOS TÉCNICOS PARA O SOFTWARE DE PROTEÇÃO DE DADOS				
4.5	A solução deverá realizar backup de Active Directory/CA 2016 ou superior.			
4.6	A solução deverá realizar backup das contas do Microsoft 365 (Teams/Sharepoint/Exchange).			
4.7	A solução deverá realizar backup de Kubernetes/Tanzu.			
4.8	A solução deverá realizar backup de máquinas virtuais VMware.			
NOTAS: <sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida; <sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes do software de proteção de dados ofertado utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos. <sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização do software de proteção de dados ofertado.				

ITEM 2 - REQUISITOS TÉCNICOS PARA O SERVIDOR DE ARMAZENAMENTO DE ALTO DESEMPENHO				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) 2	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) 3
1	SERVIDOR DE ARMAZENAMENTO DE ALTO DESEMPENHO			
1.1	Especificação Técnica			
1.1.1	Deverão ser fornecidos, juntamente com o software de proteção de dados, 04 (quatro) servidores, cada um com as seguintes características:			
1.1.2	- Deverá possuir sistema operacional Linux Red Hat Enterprise 9 ou superior licenciado para todos os processadores e cores, durante todo o período do contrato e com suporte Premium.			



ITEM 2 - REQUISITOS TÉCNICOS PARA O SERVIDOR DE ARMAZENAMENTO DE ALTO DESEMPENHO				
1.1.3	- Deverá constar no Red Hat certified hardware como servidor certificado com o sistema operacional Linux Red Hat Enterprise 9 ou superior, devendo constar no sitio da fabricante em: <a href="https://catalog.redhat.com/">https://catalog.redhat.com/</a>			
1.1.4	- Deverá possuir, no mínimo, 2 (dois) processadores para servidores corporativos das famílias Intel Xeon 6745P, de sexta geração ou superior.			
1.1.5	- Deverá possuir, no mínimo, 2048 (dois mil e quarenta e oito gigabytes) de memória RAM DDR5 ou superior, com tecnologia advanced ECC (Error-Correcting Code) ou Chipkill ou Extended ECC ou Chipspare ou tecnologia equivalente, provisionados por módulos de mesmo tamanho, na velocidade máxima e quantidades suportada pelo processador. A memória RAM deverá ser fornecida pelo FABRICANTE do equipamento, devendo ser compatível e homologada para o processador e para o modelo de servidor físico. Os módulos deverão ser distribuídos de forma a proporcionar maior desempenho, e de acordo com as boas práticas definidas pelo fabricante para o processador.			
1.1.6	- Deverá possuir fontes e ventiladores redundantes e em sua configuração máxima.			
1.1.7	- Deverá possuir 2 (dois) discos SSD de, no mínimo, 480 GB, conectados a uma controladora RAID configurada em RAID-1.			
1.1.8	- Deverá possuir módulo TPM (Trusted Platform Module) 2.0 ou superior instalado.			
1.1.9	- Deverá possuir modulo de gerenciamento (iDrac, ILO, ILOM ou similar), com todas as funcionalidades devidamente licenciadas, permitindo o suporte a gerenciamento remoto da solução.			
1.1.10	- Deverá possuir, no mínimo, 4 (quatro) interfaces 10/25GbE, em dois adaptadores de rede diferentes.			
1.1.11	- Deverá possuir, no mínimo, 2 (duas) interfaces 40 GbE , em dois adaptadores de rede diferentes.			
1.1.12	- Deverá possuir, no mínimo, 2 (duas) interfaces 100 GbE , em dois adaptadores de rede diferentes.			

ITEM 2 - REQUISITOS TÉCNICOS PARA O SERVIDOR DE ARMAZENAMENTO DE ALTO DESEMPENHO				
1.1.13	- Caso o FABRICANTE possua interfaces de rede 40/100 GbE com a velocidade determinada pela GBICs, será aceita a entrega da mesma quantidade de interfaces, ou seja 4 (quatro) com 2 GBICs de 40 GbE e 2 GBICs de 100 GbE, em adaptadores diferentes. Em substituição aos itens 1.1.11 e 1.1.12			
1.1.14	- Deverão ser fornecidos GBICs do mesmo fabricante do servidor em quantidade e velocidades iguais as interfaces para todas as portas LAN.			
1.1.15	- Deverão ser fornecidos os respectivos cordões óticos do tipo OM4 LC/UPC - LC/UPC de 3 metros para as todas as portas 10/25 GbE e cordões óticos de 15 metros do tipo MPO 12 em igual quantidade ao número de portas 40/100 GbE.			
1.1.16	- Para a conexão dos equipamentos com a rede do TJPR deverão ser fornecidos 16 (dezesesseis) GBICs da marca Cisco no modelo 10GBaseSR CISCO-FINISAR part number FTLX8571D3BCL-C3			
1.1.17	- Deverá possuir, no mínimo, 2 (duas) interfaces 32 Gbps fiber channel, em dois adaptadores diferentes, em conjunto com os respectivos GBICs e cabos óticos de no mínimo 5 metros.			
1.1.18	- Deverá possuir, no mínimo, 20 discos SSD ligados a arquitetura NVME de no mínimo 7,68 TB cada.			
1.1.19	- BIOS deverá possuir opção de criação de senha de acesso, senha de administrador ao sistema de configuração do equipamento.			
1.1.20	- Chassi montável em rack padrão 19 com altura máxima de 2U.			
1.1.21	- Garantia, subscrição e suporte técnico de no mínimo 60 meses.			
1.1.22	- A CONTRATADA deverá fornecer componentes de infraestrutura e serviços de instalação e ativação, para realização dos ajustes elétricos, instalação de novos pontos de energia, disjuntores, cabos, entre outros, no ambiente do Data Center Corporativo do Estado, necessários à instalação da solução fornecida.			

ITEM 2 - REQUISITOS TÉCNICOS PARA O SERVIDOR DE ARMAZENAMENTO DE ALTO DESEMPENHO				
1.1.23	- Acordo de Nível de Serviço (ANS) de 6 horas de solução fornecido pelo FABRICANTE do servidor. A PROPONENTE deverá detalhar o presente item descrevendo o PART NUMBER da garantia do FABRICANTE da solução que está sendo ofertada.			
<p>NOTAS:</p> <p><sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;</p> <p><sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes do software de proteção de dados ofertado utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.</p> <p><sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização do software de proteção de dados ofertado.</p>				

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) <sup>2</sup>	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) <sup>3</sup>
1	APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE			
1.1	Características Gerais			
1.1.1	Deverão ser entregues 2 (dois) equipamentos, os quais devem obrigatoriamente fazer uso de sistemas de armazenamento de alta densidade backup em disco, baseado em “appliance”, que se entende como um subsistema com o propósito específico de ingestão dos dados de backup, deduplicação e replicação.			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.1.2	Cada "Appliance" ou "solução composta de equipamentos" deverá ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de ingestão, deduplicação e replicação dos dados enviados pelos servidores de backup.			
1.1.3	Entende-se por deduplicação dos dados, a funcionalidade que permite eliminar segmentos redundantes e compactar os dados, de forma a reduzir a capacidade de disco destinada ao armazenamento dos dados de backup.			
1.1.4	Cada equipamento ou a solução composta pelos equipamentos ofertados devem ter capacidade mínima nativa de armazenamento em disco de no mínimo 500 TB (Terabytes) líquidos, instalados e licenciados, descontadas todas as perdas com redundâncias (RAID e Hot-Spares) e ganhos com compactação e/ou deduplicação, archiving e outras tecnologias que possam influenciar na capacidade mínima exigida.			
1.1.5	Deverá suportar movimentação/tierização automatizada de dados deduplicados para repositório de retenção de longo prazo, que poderá ser implementado em objeto compatível com protocolo S3 ou em repositório de retenção nativo do próprio fabricante, desde que deduplicado.			
1.1.6	Deverá fazer uso de deduplicação Global, realizando a redução de dados entre todos os protocolos de ingest. Os dados armazenados no repositório de retenção de longo prazo (S3 ou repositório nativo) também devem contar com deduplicação global.			

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.1.7	Deverão fazer parte da proposta todas as licenças necessárias para utilização de 1 PB de cloudtier (espaço em object storage compatível via protocolo S3), com o objetivo de realização automatizada de tierização de dados de longa retenção para repositório baseado em S3. Para quem utiliza repositório nativo (tier interno) deverá ser entregue 50% a mais de armazenamento no item 1.1.4			
1.1.8	O equipamento ofertado, considerado em sua solução completa (podendo ser composta por múltiplos appliances em arquitetura scale-out), deve escalar a, no mínimo, 1,04 PB (Petabytes) de capacidade líquida em um único pool de deduplicação, sem considerar arquivamento ou utilização de tiers externos para extensão de capacidade.			
1.1.9	O appliance ou a solução composta pelos equipamentos ofertados ofertado em sua configuração ofertada não deverá ultrapassar 20 U's de espaço em rack.			
1.1.10	O appliance ou a solução composta deverá ter uma camada de alta performance equivalente a, no mínimo, 10 TB por appliance, contudo poderá ser aceita capacidade diferente ou a inexistência desta, desde que o fabricante comprove, em documentação oficial, que a solução atende ao desempenho mínimo do item 1.1.17 na configuração ofertada.			
1.1.11	O Appliance ou a solução composta pelos equipamentos ofertados e seus componentes (hardware e softwares) deverão ser novos, sem utilização anterior, em linha de fabricação e sem anúncio da ou com end-of- life ou end-of-support anunciado na data da entrega. Esta comprovação deve fazer parte da proposta apresentada pela contratada para análise da equipe técnica da CONTRATANTE.			
1.1.12	Não serão aceitos equipamentos ou a solução composta por equipamentos usados, remanufaturados ou de demonstração.			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.1.13	Deverá possuir no mínimo 4 (quatro) interfaces LAN 10/25 GbE, bem como deverá ser fornecido seus respectivos GBICs e cordões óticos do tipo OM4 LC/UPC - LC/UPC de 3 metros, para dados e gerência e gravação de backups via LAN;			
1.1.14	Deverá possuir no mínimo 2 (duas) interfaces LAN 40/100 GbE ou 100 GbE, bem como bem como deverá ser fornecido seus respectivos GBICs e cordões óticos do tipo MPO12 de 15 metros, para dados e gerência e gravação de backups via LAN; Caso o appliance do fabricante não possua interfaces LAN 40/100 GbE ou 100 GbE, deverá ser entregue o dobro dos componentes requeridos no item 1.1.13, contudo fica mantida a exigência de entrega dos cabos óticos do tipo MPO12 de 15 metros.			
1.1.15	Opcionalmente, será aceito o fornecimento de no mínimo 2 (duas) interfaces SAN 16 Gbps, bem como deverá ser fornecido seus respectivos GBICs, para dados e gravação de backups via SAN;			
1.1.16	Deverá possuir no mínimo 01 (Uma) interface LAN 1 Gb Ethernet com conectores RJ45, para dados e gerência e gravação de backups via LAN;			
1.1.17	O equipamento ou a solução composta pelos equipamentos ofertados deverão ter desempenho mínimo sem uso de aceleradores de 20,4 TB/hora em pelo menos um dos protocolos modos/protocolos definidos no item 1.1.20.			
1.1.18	O equipamento ofertado deve utilizar discos com proteção não inferior a RAID 6 ou tecnologia que forneça segurança e performance equivalentes ao RAID 6 (com no máximo quatorze discos por grupo) e em conjunto com área de "Hot Spare" fornecer proteção dos dados e performance de acordo com as informações técnicas do equipamento disponíveis publicamente.			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.1.19	Caso a Solução não possua “HOT-Spare” ou funcionalidade equivalente. A proponente deverá fornecer um appliance extra com as mesmas características do appliance original para fins de replicação, garantindo o acesso e a integridade dos dados.			
1.1.20	Capacidade de operação e suporte comprovado nos seguintes modos/protocolos simultaneamente: - VTL – Emulação de Tape Libraries, Drives e Cartuchos de fitas ou OST – OpenStorage Technology; - NAS – Através de protocolos CIFS e NFS, quando não suportado OST;			
1.1.21	Tecnologia de deduplicação com as seguintes características: - Deduplicação em tempo real (In Line) dos dados recebidos para gravação em disco; - Deduplicação dos dados recebidos de múltiplas instâncias de OST ou VTL e os protocolos CIFS, NFS; - Compressão de dados após a deduplicação para armazenamento em disco;			
1.1.22	Método de deduplicação baseado em comparação de blocos de dados com tamanho variável;			
1.1.23	Caso o equipamento não suporte o protocolo OST, cada cartucho de fita emulado deverá alocar dinamicamente espaço em disco equivalente ao volume de dados recebido, não podendo pré-alocar a capacidade integral da fita;			
1.1.24	Deverá efetuar deduplicação global, ou seja, um único pool de deduplicação por sistema, deduplicando assim de forma global todos os dados oriundos de qualquer protocolo (CIFS, NFS, OST, VTL), cliente e/ou aplicação;			
1.1.25	Caso não suporte deduplicação global, deverá ser acrescida área adicional de 10% da área útil total solicitada;			
1.1.26	O equipamento ou a solução composta pelos equipamentos ofertados deverão permitir a operação de forma simultânea com todos os protocolos requeridos no item 1.1.20.			

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.1.27	A deduplicação deve segmentar automaticamente os dados em blocos de tamanho variável.			
1.1.28	Deverá habilitar a deduplicação em toda a área de armazenamento ofertada.			
1.1.29	A funcionalidade de deduplicação de dados deverá ser executada em linha (in-line) ou de forma adaptativa e paralela (post-process) com a ingestão dos dados e replicação.			
1.1.30	A deduplicação poderá acontecer antes ou depois dos dados serem gravados nos discos do appliance, contudo em nenhum dos casos poderão afetar a janela de backup e a performance de ingestão mínima exigida no item 1.1.17.			
1.1.31	Deve possuir e estar licenciado para armazenamento de dados criptografados sem que exista impacto na performance do equipamento ofertado.			
1.1.32	Caso exista impacto em performance requisitada no item 1.1.17 após a habilitação e execução de criptografia dos dados armazenados, o requerimento mínimo de performance deverá ser de 50% a mais da performance definida no mesmo item;			
1.1.33	Deve possuir software de replicação totalmente licenciado para a capacidade de armazenamento do appliance			
1.1.34	Deve replicar sobre link IP permitindo o ajuste de banda de replicação dinâmico e automatizado através de programação via interface de administração.			
1.1.35	Capacidade de replicação dos dados deduplicados com outro equipamento idêntico, através de rede TCP/IP;			
1.1.36	Deve verificar constantemente e automaticamente a integridade dos dados armazenados, de forma nativa, não sendo aceito a customização de scripts para esta funcionalidade.			
1.1.37	Caso o equipamento não suporte o protocolo OST, deverá ter a capacidade de emular um mínimo de 512 drives LTO no mesmo equipamento na modalidade VTL e 128 Shares na modalidade NAS;			



### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.1.38	Caso o equipamento ou a solução composta pelos equipamentos ofertados não suporte o protocolo OST, deverá ter a capacidade de cada partição emular um mínimo de 61.000 cartuchos virtuais de fita LTO;			
1.1.39	Deverá prover através de interface WEB acesso aos seguintes dados: - Informações dos discos e/ou raid groups; - Informações das interfaces LAN e Fibre Channel; - Utilização da capacidade física e lógica (antes e após deduplicação e compressão); - Taxa de deduplicação;			
1.1.40	Deverá possuir capacidade para a detecção de falhas abrangendo auto monitoração, geração de logs, envio de e-mails e geração de traps SNMP;			
1.1.41	Deverá realizar "call-home" via WEB ou e-mail em caso de falhas, acionando automaticamente o fabricante ou a empresa responsável pela manutenção;			
1.1.42	Deverão estar incluídos softwares para configuração, gerenciamento, monitoração, todos compatíveis com Windows/Linux e licenciado para a capacidade solicitada do equipamento;			
1.1.43	O proponente deve realizar toda a instalação/integração do equipamento de deduplicação ofertado ao sistema de backup atualmente sendo utilizado.			
1.1.44	A manutenção do equipamento ou a solução composta pelos equipamentos ofertados deverão ser de responsabilidade do fabricante podendo ser prestada pelo próprio ou por empresa credenciada para tal;			
1.1.45	A solução ofertada deve contemplar o hardware e o(s) software(s) acima descritos, sua instalação física e lógica, sua ativação, configuração e testes para garantir o pleno funcionamento de toda solução;			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.1.46	Alimentação: No mínimo 2 (duas) fontes de alimentação redundantes de tensão elétrica nominal de até 240 V (duzentos e quarenta volts) AC a 60 Hz (sessenta hertz). As Fontes devem funcionar em paralelo de modo que no caso da falha de uma delas (ou grupo delas) a(s) restante(s) assumam toda a alimentação do sistema sem prejuízos ao seu correto funcionamento, As fontes que compõem a solução devem permitir a sua adição e substituição, sem interromper o funcionamento do sistema de armazenamento (HOT PLUG ou HOT SWAP);			
1.1.47	Caso haja qualquer limitação em relação à alimentação do Rack e/ou PDU's (Power Distribution Units) e componentes que integram, estes deverão ser devidamente adaptados pela PROPONENTE ao data center em que serão instalados, sem custos adicionais, de modo que sejam colocados em operação em perfeito funcionamento.			
1.1.48	Possuir integração com os softwares de backup padrões de mercado como Veeam Backup, Coomvault e Veritas devendo suportar a utilização dos respectivos mídias server.			
1.1.49	O equipamento ou a solução composta pelos equipamentos ofertados para armazenamento de alta densidade - Appliance deverão ser ofertados em rack próprio ou homologado pelo FABRICANTE. O correto dimensionamento, fornecimento e instalação da solução será de responsabilidade da contratada. Para isto a Proponente poderá realizar vistoria técnica nas instalações do Data Center da CONTRATANTE através do agendamento com o Pregoeiro e/ou Equipe de Apoio;			
1.1.50	Todos os ajustes e equipamentos necessários para o pleno funcionamento do equipamento ou da solução nos ambientes de datacenter, correrão por conta da CONTRATADA.			

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.1.51	O licenciamento das funcionalidades previstas neste item deverá ser fornecido de forma perpétua, garantindo que todos os recursos permaneçam disponíveis independentemente do término do contrato, da garantia ou do suporte.			
1.2	Garantia de hardware e software			
1.2.1	A CONTRATADA deverá ofertar serviços proativos e reativos do FABRICANTE para manter a disponibilidade da solução, incluindo os serviços de “call-home” para abertura de forma proativa de chamados e/ou envio de informações da saúde do ambiente. Os dispositivos necessários para a implementação da funcionalidade de “call-home” são de responsabilidade da CONTRATADA. Caso haja necessidade de Intervenções técnicas presenciais decorrentes de problemas técnicos nos equipamentos, quando não atendidos pelo fabricante, serão de responsabilidade da CONTRATADA;			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.2.2	<p>A garantia ofertada, incluindo serviços de manutenção de hardware “on-site” e suporte técnico, prestada pelo FABRICANTE de serviços autorizado que deverá prover atendimento ininterrupto, para a solução de problemas, seja definitiva ou de contorno. Os graus de severidade e prazos para solução de problemas são:</p> <ul style="list-style-type: none"> <li>- Grau 1: o equipamento, acessório, periférico ou camada lógica apresenta pane, falha ou não conformidade técnica que o torna total ou parcialmente inoperante. A solução técnica, definitiva ou de contorno, não poderá exceder a 6 (seis horas), contadas do chamado técnico;</li> <li>- Grau 2: o equipamento, acessório, periférico ou camada lógica apresenta pane, falha ou não conformidade técnica que prejudica a operação, uso ou acesso de função(os) básica(s). A solução técnica, definitiva ou de contorno, não poderá exceder a 24 (vinte e quatro horas), contadas do chamado técnico;</li> <li>- Grau 3: o equipamento, acessório, periférico ou camada lógica apresenta pane, falha ou não conformidade técnica que causa restrições de operação de funções acessórias. A solução técnica, definitiva ou de contorno, não poderá exceder a 48 (quarenta e oito horas), contadas do chamado técnico;</li> <li>- Grau 4: o usuário técnico da contratante apresenta dúvidas sobre instalação, configuração, customização, otimização, operacionalização, uso e administração da solução ofertada. A solução técnica, definitiva ou de contorno, não poderá exceder a 72 (setenta e duas horas), contadas do chamado técnico.</li> </ul>			
-------	--	--	--	--

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.2.3	<p>Deverá ser ofertada garantia incluindo serviços de manutenção de hardware "on-site", atualização de firmware "on-site" ou "remoto", suporte técnico e atualização de releases de software, prestada pelo FABRICANTE ou PROVEDOR AUORIZADO pelo fabricante da solução, por um período mínimo de 60 meses 24x7 (vinte quatro horas por dia, sete dias por semana), para todos os equipamentos ofertados na solução, com tempo máximo de atendimento de acordo com o grau de severidade. Para atividades de atualização de firmware on-site deverá sempre haver a presença de técnico especializado do fabricante no site da CONTRATANTE, mesmo que estas atividades sejam executadas por técnicos do fabricante de forma remota.</p> <p>- A PROPONENTE deverá detalhar o presente item descrevendo o PART NUMBER da garantia do FABRICANTE da solução que está sendo ofertada.</p> <p>- A CONTRATADA deverá apresentar a comprovação da aquisição da garantia junto ao FABRICANTE da solução, incluindo o PART NUMBER e serviços descritos no presente item no momento da entrega da solução;</p>			
1.2.4	<p>Os serviços de garantia poderão ser solicitados mediante a abertura de chamado de hardware ou software (dúvidas ou problemas), efetuado por técnicos da CONTRATANTE ou da CONTRATADA, via chamada telefônica local, DDD a cobrar ou DDG (0800), ou por e-mail, ou por formulário próprio na Internet, ao FABRICANTE, a qualquer hora do dia e em qualquer dia da semana, inclusive sábados, domingos e feriados durante todos os dias do ano (24x7x365);</p>			
1.2.5	<p>Deverão ser disponibilizados recursos para acesso online, via World Wide Web, a serviços personalizados para o Sistema de Armazenamento em Appliance proposto, como bases de conhecimento, manuais, ferramentas, entre outros;</p>			

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.2.6	Disponibilização de acesso on-line via World Wide Web ao histórico dos relatórios de chamados e atendimentos técnicos proativos e reativos;			
1.2.7	A atualização tecnológica dos softwares que compõem a solução deverá ser fornecida e implementada pelo FABRICANTE da solução, por 60 meses, sem custos para a CONTRATANTE, no prazo máximo de 90 (noventa) dias corridos a partir do seu lançamento.			
1.2.8	A CONTRATADA deverá fornecer garantia de atualização proativa de patches de correções dos sistemas operacionais ofertados, bem como a divulgação de problemas e soluções conhecidas;			
1.2.9	A CONTRATADA deverá detalhar o presente item descrevendo o PART NUMBER da garantia do FABRICANTE da solução que está sendo ofertada.			
1.3	Infraestrutura			
1.3.1	A CONTRATADA deverá fornecer componentes de infraestrutura e serviços de instalação e ativação, para realização dos ajustes elétricos, instalação de novos pontos de energia, disjuntores, cabos, entre outros, no ambiente do Data Center Corporativo do Estado, necessários à instalação da solução fornecida. Para soluções do tipo scale-out ou em cluster, a CONTRATADA deverá fornecer, para cada datacenter dedicado, um switch multigigabit com capacidade mínima de 24 portas 10 GbE+/25 GbE, com VLANs e QoS devidamente configurados, interligado à rede da CONTRATANTE por, no mínimo, dois uplinks de 25 GbE.			

### ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE

1.3.2	Deverão ser fornecidos todos os equipamentos, materiais e acessórios necessários à completa instalação, montagem e ativação da infraestrutura. Ou seja, a CONTRATADA será integralmente responsável por todos os custos relacionados à infraestrutura física e lógica — incluindo, mas não se limitando a racks, alimentação elétrica, cabeamento metálico e óptico, switches adicionais (quando em arquitetura scale-out ou cluster), portas de rede, configuração de VLAN/QoS e testes de conectividade — necessários à instalação da solução, à interconexão entre seus componentes e à sua integração com o ambiente existente da CONTRATANTE, sem qualquer ônus adicional.			
1.3.3	Deverão ser fornecidos todas as documentações e manuais técnicos necessários à manutenção e operação dos equipamentos e da infraestrutura implantada. A documentação e manuais técnicos deverão estar em Português ou Inglês.			
1.3.4	Os equipamentos, materiais e componentes fornecidos e instalados deverão ser novos e sem qualquer tipo de uso.			
1.3.5	Os equipamentos, dispositivos e materiais similares fornecidos, quando possível, deverão ser do mesmo FABRICANTE, para garantir a completa interoperabilidade entre eles.			
1.3.6	Previamente ao fornecimento, instalação e ativação da infraestrutura, deverá ser elaborado e fornecido projeto executivo completo. Após a instalação, o projeto deverá ser atualizado com a entrega, para a contratante, do “as-built”.			
1.3.7	Cabe à PROPONENTE a verificação (testes) das condições físicas de instalação, fornecidas ou existentes, para a ativação dos componentes da solução a ser fornecida, sendo está de sua responsabilidade.			

ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.3.8	A instalação de qualquer equipamento, material, dispositivo ou componentes da solução deve prever a aplicação de todas as correções publicadas e divulgadas pelo FABRICANTE.			
1.3.9	As instalações devem ser projetadas em estrito atendimento às normas Técnicas, visando garantir o perfeito funcionamento dos componentes do sistema e a integridade física dos seus usuários.			
1.3.10	Para o aceite, a infraestrutura e seus componentes serão submetidos, a critério da CONTRATANTE, a testes de desempenho e/ou demonstrações de funcionamento pela proponente contratada, que deverá demonstrar funções e parâmetros especificados neste Objeto Técnico e de Normas Técnicas, exceto por casos em que o limitante sejam componentes da infraestrutura da CONTRATANTE.			
1.3.11	O correto dimensionamento, fornecimento e instalação da infraestrutura será responsabilidade da contratada.			
1.3.12	Deverá atender às prescrições previstas nas normas ABNT ou IEC e demais normas aplicáveis.			
1.3.13	Todas as partes metálicas deverão ser corretamente aterradas.			
1.3.14	O equipamento ou a solução composta pelos equipamentos ofertados para Appliance de armazenamento de alta densidade deverão ser ofertado em rack próprio ou homologado pelo FABRICANTE. O correto dimensionamento, fornecimento e instalação da solução será de responsabilidade da contratada. Para isto a Proponente poderá realizar vistoria técnica nas instalações do Data Center da CONTRATANTE através do agendamento com o Pregoeiro e/ou Equipe de Apoio;			
1.4	Segurança			



ITEM 3 - REQUISITOS TÉCNICOS PARA APPLIANCE DE ARMAZENAMENTO DE ALTA DENSIDADE				
1.4.1	O equipamento ou a solução compostas pelos equipamentos deverão possuir funcionalidade de proteção contra exclusão e modificação de dados de backup antes do prazo de retenção pré-estabelecido, por meio de mecanismo de imutabilidade lógica (como WORM, time-lock, air-gap lógico ou equivalente), implementado de forma nativa pelo fabricante.			
<p>NOTAS:</p> <p><sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;</p> <p><sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.</p> <p><sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.</p>				

ITEM 4 - REQUISITOS TÉCNICOS PARA O INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DOS JOBS				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) <sup>2</sup>	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) <sup>3</sup>
1	INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO			
1.1	Características Gerais dos serviços			
1.1.1	O proponente deverá fornecer Gerente de Projetos (Project Manager - PM) certificado de seu próprio quadro de funcionários para coordenar as fases de planejamento, instalação, configuração e migração dos dados.			
1.1.2	O proponente deverá fornecer profissional(is) técnico certificado nos itens 1, 2 e 3 a nível de arquitetura ou superior, de seu próprio quadro de funcionários ou vinculados a CONTRATADA para coordenar tecnicamente as fases de planejamento, instalação, configuração e migração dos dados, contudo a responsabilidade sempre recairá sobre a CONTRATADA.			

ITEM 4 - REQUISITOS TÉCNICOS PARA O INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DOS JOBS				
1.1.3	A fase de planejamento deverá avaliar minimamente, os seguintes critérios: 1. Levantamento dos requisitos do negócio; 2. Levantamento dos requisitos técnicos; 3. Avaliação do ambiente atual; 4. Avaliação dos <i>jobs</i> existentes; 5. Identificação de problemas ou limitações da solução atual que precisam ser endereçados na nova solução; 6. Desenho da Nova infraestrutura, contendo o planejamento para os repositórios e configurações de segurança; 7. Workshops das tecnologias que serão implantadas para a equipe interna da CONTRATADA; 8. Cronograma de execução; 9. Desenvolver o Plano de Instalação, Plano de Configuração e Plano de Migração; 10. Ser iniciada em até 30 dias úteis a partir da assinatura do contrato; 11. Ser finalizada em até 20 dias úteis a partir do início das atividades desta fase;			
1.1.4	Toda a documentação gerada na fase de planejamento deverá ser entregue ao CONTRATANTE para compor a documentação técnica da solução.			
1.1.5	O proponente deverá indicar funcionário(s) certificados a nível de arquitetura ou superior nos itens 1,2 e 3 para executar a instalação, configuração e migração dos <i>jobs</i> , seguindo o Plano de Implantação e Migração gerado na fase de planejamento.			
1.1.6	As fases de instalação e configuração deverá ser iniciada conforme definido na DINAMICA DA EXECUÇÃO e deverão seguir o plano de Instalação e Configuração definidos na fase de planejamento.			
1.1.7	A fase de migração dos <i>jobs</i> deverá ser iniciada a partir da entrega das fases de instalação e configuração, bem como o plano de Migração.			
1.1.8	Concluindo-se a execução dos itens deste os planos deverão ser incluídos no Relatório final de implementação e entregue a equipe técnica do Tribunal de Justiça do Estado do Paraná.			
<p>NOTAS:</p> <p><sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;</p> <p><sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.</p> <p><sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.</p>				

#### ITEM 5 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO NO SOFTWARE DE PROTEÇÃO DE DADOS

ITEM 5 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO NO SOFTWARE DE PROTEÇÃO DE DADOS				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) 2	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) 3
1	CAPACITAÇÃO ARMAZENAMENTO DE ALTA DENSIDADE			
1.1	Características Gerais			
1.1.1	Capacitar até 12 participantes na instalação, configuração, operação e boas práticas de utilização de appliances de backup, garantindo segurança e eficiência na proteção de dados.			
1.1.2	Público-alvo: Profissionais da área de Tecnologia da Informação com conhecimentos básicos em infraestrutura e backup.			
1.1.3	Carga horária mínima: 60 horas.			
1.1.4	Duração diária: Até 5 horas por dia.			
1.2	Requisitos Técnicos mínimos referente ao conteúdo			
1.2.1	Introdução ao software de proteção de dados - Conceitos de backup e restore. - Arquitetura e componentes do software.			
1.2.2	Instalação e configuração inicial - Pré-requisitos do ambiente. - Parametrização e integração com sistemas existentes.			
1.2.3	Criação e gerenciamento de políticas de backup - Tipos de backup (full, incremental, diferencial). - Criação de jobs. - Testes de restauração. - Estratégias de retenção. - Agendamento e automação.			
1.2.4	Procedimentos de restauração (restore) - Recuperação completa e granular. - Testes de integridade e validação.			

ITEM 5 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO NO SOFTWARE DE PROTEÇÃO DE DADOS				
1.2.5	Gerenciamento de armazenamento e retenção - Estratégias para otimização de espaço. - Políticas de retenção e descarte seguro.			
1.2.6	Segurança e conformidade - Criptografia de dados em trânsito e em repouso. - Controle de acesso baseado em funções (RBAC). - Adequação à LGPD e normas aplicáveis.			
1.2.7	Monitoramento e relatórios - Dashboards e alertas. - Geração de relatórios para auditoria.			
1.2.8	Resolução de problemas (troubleshooting) - Diagnóstico de falhas comuns. - Procedimentos para recuperação rápida. - Ferramentas de diagnóstico. - Resolução de falhas comuns.			
1.2.9	Boas práticas e recomendações - Estratégias de backup para ambientes críticos. - Planejamento de Disaster Recovery.			
1.3	Requisitos do Instrutor			
1.3.1	Instrutor certificado e com experiência comprovada em appliances de backup.			
1.3.2	Material didático atualizado (digital ou impresso).			
1.3.3	Emissão de certificado de participação para cada aluno.			
1.3.4	Disponibilidade para ministrar o treinamento in company ou remoto, conforme necessidade do órgão.			
1.3.5	Suporte pós-treinamento por período mínimo de 30 dias.			
1.4	Requisito de aceitação			
1.4.1	Caso a maioria dos participantes do curso avaliem a capacitação como inadequado, o TJPR poderá solicitar a reaplicação da capacitação.			
1.4.2	Caso a maioria dos participantes do curso avaliem o instrutor como inadequado, o TJPR poderá solicitar a substituição do instrutor ou ainda a reaplicação da capacitação.			

## ITEM 5 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO NO SOFTWARE DE PROTEÇÃO DE DADOS

### NOTAS:

<sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;

<sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.

<sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.

## ITEM 6 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO ARMAZENAMENTO DE ALTA DENSIDADE

Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) <sup>2</sup>	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) <sup>3</sup>
1	CAPACITAÇÃO ARMAZENAMENTO DE ALTA DENSIDADE			
1.1	Características Gerais			
1.1.1	Capacitar até 12 participantes na instalação, configuração, operação e boas práticas de utilização de appliances de backup, garantindo segurança e eficiência na proteção de dados.			
1.1.2	Público-alvo: Profissionais da área de Tecnologia da Informação com conhecimentos básicos em infraestrutura e backup.			
1.1.3	Carga horária mínima: 24 horas.			
1.1.4	Duração diária: Até 5 horas por dia.			
1.2	Requisitos Técnicos mínimos referente ao conteúdo			
1.2.1	Introdução aos appliances de backup - Conceitos e arquitetura. - Diferenças entre soluções físicas e virtuais.			
1.2.2	Configuração inicial e integração - Instalação e parametrização. - Integração com sistemas operacionais e ambientes virtuais.			

ITEM 6 - REQUISITOS TÉCNICOS PARA CAPACITAÇÃO ARMAZENAMENTO DE ALTA DENSIDADE				
1.2.3	Políticas de backup e recuperação - Criação de jobs. - Testes de restauração. - Estratégias de retenção.			
1.2.4	Segurança e conformidade - Criptografia de dados. - Controle de acesso. - Normas aplicáveis (LGPD e boas práticas de governança).			
1.2.5	Monitoramento e troubleshooting - Ferramentas de diagnóstico. - Resolução de falhas comuns.			
1.2.6	Boas práticas e recomendações - Estratégias de backup para ambientes críticos. - Planejamento de Disaster Recovery.			
1.3	Requisitos do Instrutor			
1.3.1	Instrutor certificado e com experiência comprovada em appliances de backup.			
1.3.2	Material didático atualizado (digital ou impresso).			
1.3.3	Emissão de certificado de participação para cada aluno.			
1.3.4	Disponibilidade para ministrar o treinamento in company ou remoto, conforme necessidade do órgão.			
1.3.5	Suporte pós-treinamento por período mínimo de 30 dias.			
1.4	Requisito de aceitação			
1.4.1	Caso a maioria dos participantes do curso avaliem a capacitação como inadequada, o TJPR poderá solicitar a reaplicação da capacitação.			
1.4.2	Caso a maioria dos participantes do curso avaliem o instrutor como inadequado, o TJPR poderá solicitar a substituição do instrutor ou ainda a reaplicação da capacitação.			

**NOTAS:**

<sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;

<sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.

<sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.

**ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS**

ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS				
Fabricante:			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) 2	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) 3
1	SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS			
1.1	Características gerais do serviço			
1.1.1	O serviço deverá ser executado por profissional(is) com graduação superior na área de TI e certificado(s) no software item 1 e no hardware item 3.			
1.1.2	O serviço deverá ser executado por profissional(is) que tenha(m) sólidos conhecimentos na utilização e gerenciamento de sistemas de armazenamento objeto e áreas de armazenamento em nuvem S3. Esses conhecimentos deverão ser comprovados a partir de certificações em armazenamento conquistados pelo Técnico Residente nos serviços de nuvens públicas Amazon AWS, Google Cloud, Microsoft Azure, Oracle Cloud Infrastructure, IBM Cloud ou Zadara Cloud.			
1.1.3	O serviço deverá ser iniciado em entre 60 (sessenta) e 80 (oitenta) dias corridos após a assinatura do contrato.			
1.1.4	O(s) profissional(is) que executará o serviço deverá(ão) participar das fases de planejamento, instalação, configuração e migração, contudo este não deverá realizar a migração dos jobs.			
1.1.5	O(s) profissional(is) que executará o serviço deverá(ão) atuar proativamente, de modo a atender aos usuários e garantir a disponibilidade e desempenho dos serviços de TI, dentro dos resultados.			

**ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS**

1.1.6	O(s) profissional(is) que executará o serviço deverá(ão) atuar proativamente buscando a automatização e melhoria contínua dos processos e atribuições sob sua responsabilidade.			
1.1.7	O(s) profissional(is) que executará o serviço deverá(ão) atender aos chamados da fila e fazer os devidos encaminhamentos e garantir o atendimento das atividades sob a responsabilidade da CONTRATADA.			
1.1.8	O(s) profissional(is) que executará o serviço deverá(ão) garantir a coordenação e a comunicação entre equipes atuando em conjunto no atendimento de todas as ocorrências sob a responsabilidade da CONTRATADA.			
1.1.9	O(s) profissional(is) que executará o serviço deverá(ão) atuar em conjunto e coordenadamente com a equipe de gestão e fiscalização do TJPR, reportando os incidentes, os problemas ou a indisponibilidade ou degradação de desempenho de serviços, bem como sugestões de melhorias nos processos e ambientes.			
1.1.10	O(s) profissional(is) que executará o serviço deverá(ão) realizar todas as atividades típicas da sua área, mesmo aquelas não explicitamente relacionadas, bem como fazer todos os encaminhamentos, sugestões de melhorias e alinhamentos internos necessários para o atendimento das demandas junto às demais equipes da CONTRATADA ou do TJPR.			
1.1.11	O(s) profissional(is) que executará o serviço deverá(ão) comunicar qualquer incidente ou problema de segurança que coloque em risco as instalações, os serviços de TI, ativos ou as informações do TJPR.			
1.1.12	O(s) profissional(is) que executará o serviço deverá(ão) realizar a curadoria (criar, verificar, corrigir, melhorar e manter atualizados) das bases de conhecimento com scripts de solução de atendimentos, requisições, incidentes e problemas dentro da sua área.			



**ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS**

1.1.13	O(s) profissional(is) que executará o serviço deverá(ão) atuar em conjunto com a respectiva equipe de modo a manter de forma proativa os serviços de TI, ativos atualizados e em conformidade com as políticas de segurança do TJPR.			
1.1.14	Deverá prestar atendimento aos usuários do TJPR, conforme condições definidas neste TR.			
1.1.15	O(s) profissional(is) que executará o serviço deverá(ão) executar todas as atividades em concordância com as políticas de segurança da informação e de infraestrutura de TI do TJPR			
1.1.16	O(s) profissional(is) que executará o serviço deverá(ão) configurar relatórios que forneçam uma visão geral clara e atualizada sobre a saúde da infraestrutura e das aplicações da solução de proteção de dados.			
1.1.17	O(s) profissional(is) que executará o serviço deverá(ão) fornecer sugestões de melhorias e otimizações com base na análise dos relatórios de saúde da infraestrutura e das aplicações da solução de proteção de dados.			
1.1.18	O(s) profissional(is) que executará o serviço deverá(ão) apresentar e configurar novas funcionalidades que possam trazer benefícios para a operação do CONTRATANTE da solução de proteção de dados.			
1.1.19	O(s) profissional(is) que executará o serviço deverá(ão) criar visões e dashboards personalizados para o CONTRATANTE, para que a ferramenta possa monitorar efetivamente a saúde e o desempenho das operações da solução de proteção de dados.			
1.1.20	O(s) profissional(is) que executará o serviço deverá(ão) implementar e sustentar e integrações (via API), garantindo a interconexão eficiente e segura entre os sistemas da solução de proteção de dados.			
1.1.21	O(s) profissional(is) que executará o serviço deverá(ão) prover relatórios semanais de desempenho do ambiente monitorado, permitindo uma visão contínua e detalhada do estado da infraestrutura e das aplicações da solução de proteção de dados.			

**ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS**

1.1.22	O(s) profissional(is) que executará o serviço deverá(ão) desenvolver e/ou aplicar plugins conforme necessário, para personalizar e melhorar a funcionalidade do ambiente monitorado da solução de proteção de dados.			
1.1.23	O(s) profissional(is) que executará o serviço deverá(ão) executar todas as atividades relacionadas ao gerenciamento de backups e restauração. Além disso, é responsável por atender a todas as demandas que envolvem suas atribuições, bem como prestar o suporte a outras áreas de TI conforme demandado.			
1.1.24	O(s) profissional(is) que executará o serviço deverá(ão) projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de proteção de dados do CONTRATANTE.			
1.1.25	O(s) profissional(is) que executará o serviço deverá(ão) tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de backup e armazenamento do CONTRATANTE.			
1.1.26	O(s) profissional(is) que executará o serviço deverá(ão) realizar configurações, alterações e otimizações no ambiente de proteção de dados do CONTRATANTE.			
1.1.27	O(s) profissional(is) que executará o serviço deverá(ão) realizar testes de restore com definição de frequência, a critério do CONTRATANTE.			
1.1.28	O(s) profissional(is) que executará o serviço deverá(ão) manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças.			
1.1.29	O(s) profissional(is) que executará o serviço deverá(ão) acompanhar fornecedores caso necessário.			
1.1.30	O(s) profissional(is) que executará o serviço deverá(ão) elaborar e manter atualizada a documentação de todo o ambiente.			

**ITEM 7 - REQUISITOS TÉCNICOS PARA SERVIÇO DE GERENCIAMENTO TÉCNICO E SUSTENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS**

1.1.28	O(s) profissional(is) que executará o serviço deverá(ão) executar, manter, atualizar, implantar e apoiar na criação das políticas de backup do CONTRATANTE.			
--------	---	--	--	--

**NOTAS:**

<sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;

<sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.

<sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.

**ITEM 8 - REQUISITOS TÉCNICOS PARA O HORAS TÉCNICAS ESPECIALIZADAS SOB DEMANDA**

Fabricante			Modelo:	
Item	Características Mínimas Exigidas	Atendimento do Item (sim ou não) <sup>1</sup>	Descrição do Item proposto (preenchimento obrigatório) <sup>2</sup>	Documentação oficial do fabricante com indicação da página específica que comprova o respectivo item para verificação (preenchimento obrigatório) <sup>3</sup>
1	HORAS TÉCNICAS ESPECIALIZADAS SOB DEMANDA			
1.1	Características Gerais do serviço			
1.1.1	A CONTRATADA deverá fornecer até 1.000 horas técnicas, a serem utilizadas sob demanda, conforme o critério da CONTRATANTE.			
1.1.2	As horas técnicas requisitadas pelo CONTRATANTE e executadas pela CONTRATADA através de profissionais certificados pela fabricante, têm por finalidade o desenvolvimento de projetos complexos, implementação de novas funcionalidades, melhorias no software de integração, consultoria e criação de treinamentos de capacitação no objeto contratado.			

ITEM 8 - REQUISITOS TÉCNICOS PARA O HORAS TÉCNICAS ESPECIALIZADAS SOB DEMANDA				
1.1.3	Cabe ao CONTRATANTE a gestão, controle e fiscalização das horas técnicas a serem executados, e à CONTRATADA a execução operacional através do gerenciamento dos seus recursos humanos e físicos.			
1.1.4	As Hora técnicas deverão ser prestadas preferencialmente na modalidade remota.			
1.1.5	As Hora técnicas, quando forem realizados na modalidade presencial, deverão ser realizados no local onde encontra-se instalado o objeto contratado, sendo restrita à comarca de Curitiba.			
1.1.6	As horas técnicas, quando forem realizados na modalidade presencial, deverão ter a duração mínima necessária para a solução da demanda de acordo com o Horário Regimental do TJPR.			
1.1.7	As horas técnicas serão pagas sob demanda, ficando a cargo do CONTRATANTE a fiscalização, homologação e aprovação.			
1.1.8	A CONTRATADA deverá executar as horas técnicas através de profissional devidamente qualificado na tecnologia do serviço executado.			
1.1.9	A CONTRATADA deverá realizar análise de problemas e incidentes, a fim de garantir uma resolução rápida e eficaz para manter a operação do CONTRATANTE sem interrupções.			
1.1.10	A CONTRATADA deverá realizar reuniões periódicas para avaliar o ambiente monitorado, discutir problemas identificados e planejar atividades futuras.			
1.1.11	A CONTRATADA fornecerá atualização e treinamento para as equipes do CONTRATANTE, garantindo que estejam totalmente alinhadas para usar eficientemente todas as funcionalidades do objeto contratado.			
1.1.12	A CONTRATADA realizará workshops, quando necessário, para orientar e educar as equipes do CONTRATANTE sobre as melhores práticas e novas funcionalidades da solução.			
1.2	REQUISITOS DO CONTROLE DOS SERVIÇOS TÉCNICOS ESPECIALIZADOS			

**ITEM 8 - REQUISITOS TÉCNICOS PARA O HORAS TÉCNICAS ESPECIALIZADAS SOB DEMANDA**

1.2.1	A gestão das horas técnicas deverá ser realizada pelo servidor designado para o projeto, com o apoio do Departamento de Tecnologia da Informação e Comunicação, da área demandante e gestor do contrato do CONTRATANTE.			
1.2.2	A solicitação do serviço técnico especializado será realizada através de ordem de serviço emitida pelo CONTRATANTE.			
1.2.3	O CONTRATANTE deverá elaborar a ordem de serviço e encaminhar a ordem de serviço para a CONTRATADA para fins de orçamentos e quantificação dos recursos necessários ao projeto.			
1.2.4	A CONTRATADA deverá confirmar o recebimento da ordem de serviço no prazo máximo de 01 dia útil contado da comunicação pelo CONTRATANTE (SLA1).			
1.2.5	A CONTRATADA deverá analisar a ordem de serviço e elaborar o plano de trabalho com cronograma de execução em relação às demandas a serem atendidas com a solicitação no prazo máximo de 10 dias úteis, contados a partir da resposta a CONTRATANTE e 3 dias úteis a partir da recusa da execução da ordem de serviço (SLA2).			
1.2.6	O CONTRATANTE poderá aprovar, reprovar ou cancelar o plano de trabalho e a execução da ordem de serviço.			
1.2.7	No caso de aprovação a CONTRATADA deverá: (SLA3) - Executar a ordem de serviço de acordo com a quantidade de horas técnicas e o valor definidos no aceite da ordem de serviço e; - Executar a ordem de serviço de acordo com o plano de trabalho e cronograma de execução aprovado.			
1.2.8	Em caso de irregularidade na execução da demanda, a CONTRATADA deverá solucionar todas as irregularidades apontadas em prazo fixado pelo CONTRATANTE. (SLA4)			
1.2.9	Após a aprovação da execução da ordem de serviço o CONTRATANTE emitirá o Termo de Recebimento pela execução de horas sob demanda			

## ITEM 8 - REQUISITOS TÉCNICOS PARA O HORAS TÉCNICAS ESPECIALIZADAS SOB DEMANDA

1.2.10	Por fim, em não havendo irregularidades execução da demanda, o CONTRATANTE deverá homologar o relatório final da ordem de serviço encaminhado pela CONTRATADA.			
1.2.11	Após o recebimento do Termo de Recebimento pela execução de horas sob demanda a CONTRATADA fica autorizada a solicitar o pagamento do serviço			
1.2.12	Haverá suspensão de contagem dos prazos para a ordem de serviço que, realmente for comprovado que houve alguma pendência por parte do CONTRATANTE.			
1.2.13	Em caso de atrasos nas respostas, descumprimento do cronograma ou deixar de executar o serviço definido no aceite da ordem de serviço, a CONTRATADA estará sujeita a sanção na forma prevista no Caderno de Penalizações conforme SLA infringido.			

### NOTAS:

<sup>1</sup> Responder (sim) ou (não) para a respectiva característica técnica mínima exigida;

<sup>2</sup> Característica técnica de DESCRIÇÃO OBRIGATÓRIA - As proponentes deverão apresentar as características técnicas dos componentes da solução ofertada utilizando a própria planilha, preenchendo os campos obrigatórios a elas destinados, sem alterar os campos já preenchidos.

<sup>3</sup> Anexar documentação comprobatória em papel para cada item ofertado, com indicação da página específica que comprova o respectivo item. Não serão aceitos links para verificação na Internet. A não observância do preenchimento destas características e referência documental para fins de comprovação, poderá implicar na desclassificação da proponente, por falta de elementos de caracterização da solução ofertada.



Documento assinado eletronicamente por **ERSAN RAFAEL HOLSTEIN, Técnico em Computação**, em 27/05/2026, às 15:28, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **MARCO ANTONIO GOMES BERNARDINO, Chefe da Divisão de Sustentação da Coordenadoria de Infraestrutura e Operações**, em 27/05/2026, às 15:43, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **DIOGO RODRIGO TERRA SILVEIRA, Técnico em Computação**, em 27/05/2026, às 15:55, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **MAYCON CEZAR GARCIA PENHA, Técnico em Computação**, em 27/05/2026, às 16:29, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.tjpr.jus.br/validar> informando o código verificador **13070564** e o código CRC **91614758**.