TRIBUNAL REGIONAL ELEITORAL DO DF

# ESTUDOS PRELIMINARES

**AQUISIÇÃO DE BENS E/OU SERVIÇOS DE TIC**
**(CONFORME A LEI 14.133/2021 E RES. CNJ 468/2022)**

**INTRODUÇÃO**

O Estudo Técnico Preliminar tem por objeto identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

## 1. DESCRIÇÃO DETALHADA DO OBJETIVO, COM ESPECIFICAÇÃO DOS REQUISITOS NECESSÁRIOS:

### 1.1. OBJETIVO

1.1.1. O objetivo deste estudo é a constatação da viabilidade da contratação do serviço de suporte técnico e atualização de ferramentas opcionais de *software* de segurança para bancos de dados Oracle (*options* e *packs*), a ser realizado com a empresa Oracle do Brasil Sistemas Ltda., com base no artigo 74, I, da Lei n° 14.133/2021 (inexigibilidade de licitação).

1.1.2. Para uma melhor especificação, entende-se por "*suporte e atualização de versão*", o serviço conforme definido pela Oracle, a ser prestado pelo fabricante pelo período de 60 (sessenta) meses, contados da inscrição das licenças na conta de "*Support Identifier*" do Tribunal Contratante no site do fabricante, compreendendo pelo menos:

1.1.2.1. Acesso às bases de conhecimento;

1.1.2.2. Atendimento remoto (*web* ou telefone) para chamados de suporte técnico, que podem ser abertos 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana (24 x 7), com opção de língua portuguesa;

1.1.2.3. Atualização de versão; e

1.1.2.4. Disponibilização de *patches* corretivos.

1.1.3. Os itens a serem adquiridos são os constantes da seguinte tabela:

| Item | Descrição do serviço | CATSER | Unidade de medida | Quantidade |
|---|---|---|---|---|
| 1 | Oracle Advanced Security - Processor Perpetual - Suporte Técnico | 27502 | Unidade | 4 |
| | Oracle Advanced Security - Processor Perpetual - Atualização | 27502 | | |
| 2 | Oracle Database Vault - Processor Perpetual - Suporte Técnico | 27502 | Unidade | 4 |
| | Oracle Database Vault - Processor Perpetual - Atualização | 27502 | | |
| 3 | Oracle Data Masking and Subsetting Pack - Processor Perpetual - Suporte Técnico | 27502 | Unidade | 4 |
| | Oracle Data Masking and Subsetting Pack - Processor Perpetual - Atualização | 27502 | | |

### 1.2. REQUISITOS FUNCIONAIS E NÃO FUNCIONAIS

#### 1.2.1. REQUISITOS DE NEGÓCIO:

1.2.1.1. Trata-se, resumidamente, de atender às necessidades de segurança relacionadas à análise, detecção e gerenciamento de vulnerabilidades no banco de dados Oracle no TRE-DF. A solução deverá garantir a compatibilidade de versão com o *Oracle Database Enterprise Edition* do ambiente de produção do contratante e versões advindas de atualização e correções de falhas, enquanto estiverem vigentes os serviços de suporte e atualização.

#### 1.2.2. REQUISITOS DE GARANTIA E MANUTENÇÃO:

1.2.2.1. A empresa deverá prestar serviços de suporte técnico, atualização e disponibilização de *patches* de segurança por 60 meses.

1.2.2.2. A empresa contratada deve prestar os serviços de suporte e atualização de versão, com atendimento de chamados no caso de falhas, dúvidas, atualizações e suporte, observando os seguintes aspectos:

1.2.2.2.1. Abertura de chamados técnicos se dará por intermédio de número telefônico de discagem gratuita (0800) ou internet, obedecendo aos seguintes padrões de severidade:

1.2.2.2.1.1. **Severidade 1**: O uso do sistema de programa suportado e interrompido ou tão severamente impactado que não é possível trabalhar ou operar de modo razoável. A perda do serviço é total. A operação é essencial para o negócio e trata-se de uma emergência. Uma solicitação de serviço severidade 1 tem uma ou mais das seguintes características: **A/** Dados corrompidos; **B/** Uma função crítica documentada não está disponível; **C/** O sistema trava indefinidamente, causando demoras inaceitáveis ou indefinidas para recursos ou respostas; **D/** O sistema falha repetidamente após tentativas de reinicializações.

1.2.2.2.1.2. **Severidade 2:** A perda do serviço é significativa. Funcionalidades importantes não estão disponíveis, com nenhuma alternativa aceitável; no entanto, a operação pode continuar de forma limitada.

1.2.2.2.1.3. **Severidade 3:** A perda do serviço é pequena. O problema gera inconvenientes que podem requerer uma solução temporária para restaurar a funcionalidade.

1.2.2.2.1.4. **Severidade 4:** Solicita-se informações, melhorias ou esclarecimentos relativos ao seu software, mas não há impacto na operação do mesmo. Não há perda de serviço. O resultado não impede o funcionamento do sistema.

1.2.2.2.2. Os atendimentos aos chamados técnicos devem ocorrer conforme o nível mínimo de serviço detalhado no quadro abaixo:

| Nível de severidade | Tempo máximo de resposta | Disponibilidade de atendimento |
|---|---|---|
| 1 | 90% dos chamados de severidade 1 deverão ser respondidos no prazo de 1 (uma) hora | 24 horas por dia, 7 dias por semana |
| 2 | 90% dos chamados de severidade 2 deverão ser respondidos no prazo de 2,5 (duas e meia) horas comerciais locais | 8 horas por dia, 5 dias por semana |
| 3 | 90% dos chamados de severidade 3 deverão ser respondidos no prazo do próximo dia útil local | 8 horas por dia, 5 dias por semana |
| 4 | 90% dos chamados de severidade 4 deverão ser respondidos no prazo do próximo dia útil local | 8 horas por dia, 5 dias por semana |

1.2.2.2.3. O prazo definido na tabela acima para resposta será contado da notificação da CONTRATADA pelos meios previstos no item 8.1.1 do Termo de Referência.

**1.2.3. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO**

1.2.3.1. Os serviços deverão ser executados em conformidade com as normas das Políticas e Protocolos de Segurança da Informação do Tribunal, que estão disponibilizadas no Portal da Transparência do TRE-DF - Governança de TIC (Governança de TIC — Tribunal Regional Eleitoral do Distrito Federal (tre-df.jus.br)).

1.2.3.2. A contratante não compartilhará com a contratada, sob nenhuma hipótese, base de dados que contenham dados pessoais ou dados sensíveis, mesmo que alegada necessidade para atendimento de suporte técnico.

1.2.3.3. Os serviços deverão fornecer credenciais seguras para a contratante a fim de acessar o suporte técnico e as atualizações de versão.

1.2.3.4. Os serviços deverão proporcionar a alteração da senha de acesso ao suporte técnico e às atualizações sempre que considerar conveniente, sem necessidade de anuência da contratada.

1.2.3.5. Os serviços não poderão utilizar-se das bases de dados da contratada para nenhum fim, sem o consentimento da contratante, mesmo que se trate de pesquisas não identificadas para melhoria da solução.

1.2.3.6. A contratada, tendo acesso a dados pessoais de servidores da contratante para fins de cadastro de acesso ao suporte técnico e às atualizações, deverá se comprometer a manter sigilo das informações, por meio do **Termo de Compromisso e Manutenção de Sigilo,** anexo ao Termo de Referência.

1.2.3.7. A contratada, na hipótese de vir a atuar no contrato e ter acesso ao banco de dados da contratante, deverá assinar o Termo de Compromisso de Manutenção de Sigilo, em anexo ao Termo de Referência, bem como manifestar ciência da Política de Acesso aos Recursos de TIC, bem como da Política de Gerenciamento de Crises Cibernéticas do TRE-DF.

**1.2.4. REQUISITOS TECNOLÓGICOS E DE ARQUITETURA:**

1.2.4.1. Os serviços deverão disponibilizar pelo período de vigência da contratação a atualização das licenças dos programas de segurança Oracle, visando mantê-los atualizados de acordo com as últimas versões disponibilizadas pela ORACLE, bem como através da aplicação de pacotes corretivos e evolutivos (*patches*);

1.2.4.2. Os serviços deverão oferecer suporte técnico no padrão OSS-ORACLE Suport Service, 7 (sete) dias por semana, 24 (vinte e quatro) horas por dias, aos softwares ORACLE, através de discagem telefônica gratuita, prestado diretamente pela Central de Suporte da ORACLE e suporte técnico web via portal da ORACLE.

1.2.4.3. Os serviços deverão proporcionar que a solução forneça e mantenha as credenciais de acesso ao Portal MY ORACLE SUPPORT.

1.2.4.4. Os serviços deverão disponibilizar referências e informações técnicas através da internet, com acesso pelo endereço eletrônico MY ORACLE SUPPORT (https://support.oracle.com), que inclui biblioteca eletrônica, fórum de debates, informações sobre produtos e banco de problemas/soluções.

1.2.4.5. Os serviços deverão disponibilizar, 24 (vinte e quatro) horas e 7 dias por semana, sem ônus adicionais, acesso à Base de Conhecimento Mundial sobre produtos ORACLE contemplados no objeto deste Termo.

1.2.4.6. Deverá manter a compatibilidade entre os componentes de software, garantindo o funcionamento consistente e harmonioso.

1.2.4.7. Deverá ser compatível com arquitetura *multi-tenant* e também para arquitetura *non-cdb* do Oracle Database.

**1.2.5. REQUISITOS LEGAIS:**

1.2.5.1. Os serviços deverão estar alinhados com os normativos a seguir elencados e com as boas práticas das “Referências Técnicas” consideradas para a presente contratação:

1.2.5.1.1. Os serviços deverão proporcionar que a solução proteja os dados de acessos não autorizados (Art. 6°, VII, e Art. 46 da LGPD; CNJ n° 363/2021; Res.TSE n° 23650/2021 e n° 23.644/2021).

1.2.5.1.2. Os serviços deverão proporcionar que a solução proteja os dados de situações acidentais de destruição, perda, alteração, comunicação ou difusão (Art. 6°, VI e Art. 46, I, da LGPD).

1.2.5.1.3. Os serviços deverão proporcionar que a solução prevenina a ocorrência de danos em virtude do tratamento de dados (Art. 6º, VIII, da LGPD).

1.2.5.1.4. Os serviços deverão proporcionar que a solução seja capaz de comprovar a observância e o cumprimento de normas de proteção de dados (Art. 6°, X, da LGPD, Res. TSE n° 23.650/2021).

1.2.5.1.5. Os serviços deverão proporcionar que a solução seja capaz de tornar os dados pessoais anônimos de modo não reversível (Art. 12, § 3°, e Art. 16, II e IV, da LGPD).

1.2.5.1.6. Os serviços deverão proporcionar que a solução seja capaz de manter registro de auditoria das operações de tratamento de dados (LGPD, Art. 37, II e IV; Res. TSE n° 23.650/2021).

1.2.5.1.7. Os serviços deverão proporcionar que a solução informe sobre tentativa de violação de política de segurança (LGPD, Art. 48,§ 1º; Res. TSE nº 23.650/2021, Art. 8º, VIII; Res. TSE nº 23.650/2021, Art. 15º, III, e Art. 17º, IV; Resolução nº 23.644/2021, Art. 7º, V; Resolução nº 23.644/2021, Art. 14, §2º)

1.2.5.1.8. Os serviços deverão proporcionar que a solução mantenha os registro de auditoria de tentativa de violação ou violação de política de segurança (LGPD, Art. 48, III).

1.2.5.1.9. Os serviços deverão proporcionar que a solução permita a adoção de medidas técnicas para tornar os dados ininteligíveis para terceiros não autorizados a acessá-los (LGPD, Art. 48, § 3º; TSE n° 23650/2021, Art. 14, IV).

1.2.5.1.10. Os serviços deverão proporcionar que a solução permita medidas tais como a aposição de tarjas sobre dados pessoais ou a supressão parcial de números cadastrais (TSE n° 23.650/2021, Art. 7°, Parágrafo Único).

1.2.5.1.11. Os serviços deverão proporcionar que a solução permita o uso de recursos criptográficos sobre os bancos de dados (Resolução TSE n° 23.644/2021, Art. 9º, II, e Art. 17).

1.2.5.1.12. A fabricante da solução deverá entregar cópias originais e legalizadas para instalação, atualização ou correção de falhas técnicas, em observância com a legislação pertinente à propriedade intelectual e de direitos autorais de software (Lei n° 9.279/1996 e Lei n° 9.609/1998).

**1.2.6. REQUISITOS FUNCIONAIS**

**1.2.6.1. Criptografia de dados:**

1.2.6.1.1. Os serviços deverão manter a criptografia de dados na camada de armazenamento, de forma nativa e sem necessidade de utilização de soluções de terceiros, sem impacto na interface que as aplicações usam, sem afetar comandos SQL de entrada ou saída, demandar por alterações nas aplicações clientes ou por configurações específicas de hardware, tais como filesystems criptografados.

1.2.6.1.2. Os serviços deverão manter a apresentação dos dados descriptografados, de forma transparente quando acessos por meio de SQL por usuários e aplicações autorizados pela camada de banco de dados, de forma nativa e sem necessidade de utilização de soluções de terceiros e sem demandar por alterações de código nas aplicações clientes ou por comandos ou configurações de hardware específicas, tais como filesystems criptografados.

1.2.6.1.3. Os serviços deverão manter a criptografia para arquivos de backup gerados pela ferramenta Oracle Database - Recovery Manager (RMAN), de forma nativa, sem necessidade de utilização de soluções de terceiros.

1.2.6.1.4. Os serviços deverão manter a criptografia para arquivos de export gerados pela ferramenta Oracle Database Data Pump, de forma nativa, sem necessidade de utilização de soluções de terceiros.

1.2.6.1.5. Os serviços deverão manter a escolha do tamanho da chave criptográfica e o algoritmo nas operações de criptografia, oferecendo, minimamente: 3DES168, AES128, AES192,AES256.

1.2.6.1.6. Os serviços deverão manter a capacidade de utilizar chaves criptográficas armazenadas no Oracle wallet, nos padrões PKCS#12 e PKCS#5.

1.2.6.1.7. Os serviços não deverão alterar as características da solução de incapacitar a leitura de dado textuais contidos nos datafiles quando estes forem abertos diretamente no sistema operacional, sem a mediação do Sistema Gerenciador de Banco de Dados.

1.2.6.1.8. Os serviços deverão permitir a escolha da granularidade da operação de criptografia, possibilitando, minimamente, a seleção de coluna ou tablespaces que serão criptografados.

1.2.6.1.9. Os serviços deverão permitir à solução criptografar dados em repouso, ou seja, que estejam armazenados nos arquivos de dados, nos tablespaces de dados, undo e outros arquivos dos quais o Oracle Database faça uso, tais como redo logs. Não é escopo a criptografia de dados em trânsito por meio de protocolos de comunicação.

1.2.6.1.10. Os serviços deverão permitir à solução ser completamente integrada ao Oracle Database, com suporte à aceleração de criptografia baseada em hardware, compatível com tecnologi° Intel® Advanced Encryption Standart Instruction (AES-NI).

1.2.6.1.11. Os serviços deverão permitir à solução apresentar *overhead* mínimo no atendimento às requisições de banco de dados, limitado a um acréscimo de 10% do tempo de resposta exibido em bancos idênticos, sobre infraestrutura idêntica, sem criptografia.

1.2.6.1.12. Os serviços deverão manter a solução capaz de utilizar de chaves de criptografia de padrões PKCS#12 e PKCS#5.

1.2.6.1.13. Os serviços deverão manter a solução a permitir a compressão de dados em dados criptografados.

1.2.6.1.14. Os serviços deverão manter a solução não impedir o uso de transportable tablespace para dados criptografados.

1.2.6.1.15. Os serviços deverão manter a solução não ter limitações quanto ao tipo e quanto ao tamanho do dado a ser criptografado.

1.2.6.1.16. Os serviços deverão manter a solução capaz de impossibilitar o aumento de espaço de armazenamento utilizado, em função de eventual *overhead* no processo de criptografia.

**1.2.6.2. Reescrita de dados:**

1.2.6.2.1. Os serviços deverão manter a solução, considerando as restrições de acesso definidas, a aposição de tarjas para dados selecionados ou outro mecanismo que permita ocultar todo ou parte do dado, doravante denominado de “reescrita do dado” antes da resposta à consulta.

1.2.6.2.2. Os serviços deverão manter a solução ser capaz de realizar a reescrita do dado, de forma nativa, sem a necessidade de alteração da aplicação ou o uso de ferramentas de terceiros.

1.2.6.2.3. Os serviços manterão a solução capaz de realizar a reescrita do dado, minimamente, nos seguintes modos: a) Completo: Reescreverá todo o dado. Ex.: Se o CPF for 455.821.052-39, a solução não deve exibir nenhum dígito real. b) Parcial: Reescreverá porção do dado. Ex.: Se o CPF for 455.821.052-39, parte a informação pode estar visível, como em 4XX.XXX.XXX-39. c) Por expressões regulares: Reescreverá o dado mediante casamento de padrões de texto. Ex.: reescrever parte de e-mail baseado na expressão regular do domínio. De joao@tre-df.jus.br para ***@****.jus.br d) Aleatório: Reescreverá o dado de forma aleatória a cada consulta. e) Nenhuma: Não haverá reescrita alguma sobre o dado..

1.2.6.2.4. Os serviços deverão manter a solução capaz de reescrever o dado entregue para a consulta, sem afetar o dado armazenado no Oracle Database.

1.2.6.2.5. Os serviços deverão manter a solução capaz de reescrever o dado consultado em tempo de execução.

1.2.6.2.6. Os serviços deverão manter a solução capaz de prover critérios de reescrita flexíveis, considerando o contexto da sessão do usuário de banco responsável pela consulta.

1.2.6.2.7. Os serviços deverão manter a solução capaz de permitir a criação de várias políticas de reescrita de dados.

1.2.6.2.8. Os serviços manterão a solução capaz de reescrever dados dos seguintes tipos, minimamente: a) Caracters: CHAR, VARCHAR2 (incluindo VARCHAR2 longos, por exemplo, VARCHAR2(20000)), NCHAR, NVARCHAR2; b) Dígitos: NUMBER, FLOAT, BINARY_FLOAT, BINARY_DOUBLE; c) Brutos: LONG RAW, RAW; d) Data: DATE, TIMESTAMP, TIMESTAMP WITH TIME ZONE, TIMESTAMP WITH LOCAL TIME ZONE; e) Intervalos: INTERVAL YEAR TO MONTH, INTERVAL DAY TO SECOND.

**1.2.6.3. Mascaramento de dados e Seleção de Subconjuntos de Dados:**

1.2.6.3.1. Os serviços deverão manter a solução capaz de permitir a substituição de dados sensíveis por dados falsos sem prejudicar a semântica e a estrutura dos dados, por meio de transformações sobre dados, também denominada “mascaramento de dados”, que deverá ter caráter irreversível.

1.2.6.3.2. Os serviços deverão manter a solução capaz de prover, minimamente, as seguintes transformações sobre os dados: a) Mascaramento Condicional: consiste em utilizar diferentes formatos de mascaramento a partir de condições preestabelecidas; b) Mascaramento Composto: consiste em opção de agrupamento, mascarando colunas relacionadas com um grupo, garantindo o mascaramento de dados através de colunas relacionadas (por exemplo, ao se mascarar um endereço, os campos, UF, CEP e Bairro devem estar com dados consistentes entre si); c) Mascaramento Determinístico/Consistente: consiste em gerar transformações consistentes para uma dada entrada em todas as bases de dados, mantendo a integridade entre múltiplas aplicações e preservando a integridade no ambiente utilizado (por exemplo: matrícula do servidor é utilizada por várias aplicações e deve ser mascarado consistentemente através dessas aplicações) d) Embaralhamento: consiste em transformar o dado, embaralhando-o de modo aleatório. Essa transformação auxilia na anonimização, pois quebra o relacionamento entre os dados (por exemplo, havendo o campo nome e sobrenome, executar a transformação de modo que o novo registro tenha nome não associado ao sobrenome de uma pessoa conhecida); e) Mascaramento reversível baseado em chave: consiste em criptografar e descriptografar os dados originais, utilizando uma chave segura; f) Preservação de formato aleatória: consiste na capacidade de preservar o comprimento, a posição de caracteres e números, o “case” do caractere (se maiúscula ou minúscula) e os caracteres especiais.

1.2.6.3.3. Os serviços deverão manter a solução capaz de permitir a segregação de privilégios de administração, mascaramento de dados e de criação de amostras de dados.

1.2.6.3.4. Os serviços deverão manter a solução capaz permitir o mascaramento e a produção de amostras quando em uso da ferramenta Oracle Database - Data Pump.

1.2.6.3.5. Os serviços deverão manter a solução capaz de suportar, minimamente, os seguintes tipos de dados: **Numéricos**: NUMBER, FLOAT, RAW, BINARY_FLOAT, BINARY_DOUBLE; **String**: CHAR, NCHAR, VARCHAR2, NVARCHAR2; **Data**: DATE, TIMESTAMP; **Blob**: BLOB, CLOB, NCLOB.

1.2.6.3.6. Os serviços deverão manter a solução capaz de permitir a extração de um subconjunto do universo de dados considerado, denominado de “amostra”, mantendo a integridade e consistência entre os elementos no subconjunto obtido.

1.2.6.3.7. Os serviços deverão manter a solução capaz de permitir a visualização do resultado do mascaramento e da amostra antes de efetivamente criá-los.
1.2.6.3.8. Os serviços deverão manter a solução capaz de permitir a criação de modelos que permitam a proteção da integridade dos dados durante a criação da amostra mesmo em um conjunto de dados carente de relacionamentos de integridade referencial.
1.2.6.3.9. Os serviços deverão manter a solução integrada ao Oracle Database, sem a necessidade de uso de ferramentas de terceiros.
1.2.6.3.10. Os serviços deverão manter a solução capaz de permitir que os critérios utilizados na geração de uma determinada amostra possa ser gravada, de modo que a operação possa ser repetida inúmeras vezes.
1.2.6.3.11. Os serviços deverão manter a solução capaz de prover mecanismos que auxiliem na identificação de dados sensíveis.

**1.2.6.4. Controle de Acesso:**

1.2.6.4.1. Os serviços deverão manter a solução capaz de impedir que usuários com privilégios administrativos e usuários com privilégios ANY possam vir a acessar indevidamente os dados sensíveis armazenados no banco de dados.
1.2.6.4.2. Os serviços deverão manter a solução capaz de definir regras de segurança baseadas em fatores - minimamente, IP, método de autenticação, nome do programa, atributos da sessão -, para impedir ataques originados de credenciais válidas que tenham sido roubadas.
1.2.6.4.3. Os serviços deverão manter a solução capaz de separar os papéis do administrador de políticas de segurança do papel de administrador de contas de usuários.
1.2.6.4.4. Os serviços deverão manter a solução capaz de delimitar uma zona segura dentro do banco de dados em que schemas, objetos e roles podem permanecer em segurança, a fim de que o controle de acesso seja realizado sobre essa zona segura.
1.2.6.4.5. Os serviços deverão manter a solução capaz de definir regras de segurança baseado em regras de comando (command rule) que permitiria restringir a execução de comandos SQL que incluam um conjunto de palavras-chave ou comandos DDL (database definition language) e DML (data manipulation language).
1.2.6.4.6. Os serviços deverão manter a solução capaz de agrupar várias regras de segurança em conjuntos e produzir uma avaliação única de segurança para cada conjunto que será derivado das avaliações individuais das regras que compõem o conjunto, mediante a informação dos critérios de avaliação.
1.2.6.4.7. Os serviços deverão manter a solução ser capaz de habilitar ou desabilitar roles para contas de usuário baseado na avaliação resultante do conjunto de regras.
1.2.6.4.8. Os serviços deverão manter a solução capaz de possuir uma biblioteca de funções e procedimentos que permitam ao administrador da solução flexibilidade na definição de regras de segurança.
1.2.6.4.9. Os serviços deverão manter a solução capaz de armazenar as informações de configuração, tais como zonas seguras, conjunto de regras, de forma a possibilitar consulta posterior.
1.2.6.4.10. Os serviços deverão manter a solução capaz de garantir compatibilidade com as demais funcionalidades de segurança que tratam de criptografia, mascaramento de dados e reescrita de dados.

**1.2.7. REQUISITOS DE CAPACITAÇÃO**

1.2.7.1. Os serviços deverão estar acompanhados de documentação elaborada na forma de guias de utilização, contendo informações de nível básico ao avançado.
1.2.7.2. Os serviços deverão contar com equipe capacitada no suporte técnico ao contratante, minimamente na versão instalada e também para as versões para os quais a fabricante mantenha suporte durante a vigência contratual.

**1.2.8. REQUISITOS AMBIENTAIS**

1.2.8.1. Os serviços deverão se conformar ao ambiente tecnológico e físico que está em operação na contratante.
1.2.8.2. Os serviços devem atuar na camada de banco de dados sem comprometer o desempenho dos bancos de dados da contratante.
1.2.8.3. Os serviços, as atualizações evolutivas e/ou corretivas devem ser distribuídas de forma digital e on-line, sempre que disponíveis.

**1.2.9. REQUISITOS CULTURAIS**

1.2.9.1. Os serviços não deverão implicar na alteração de nenhuma das ferramentas já utilizadas para a administração de banco de dados Oracle utilizadas atualmente.
1.2.9.2. Os serviços deverão priorizar o idioma Português Brasil sempre que possível e na sua ausência, o idioma Inglês (EUA).

**1.2.10. REQUISITOS SOCIAIS**

1.2.10.1. Os serviços não deverão impedir o exercício das funções do contratante ou gerar indisponibilidade.

**1.2.11. REQUISITOS DE MANUTENÇÃO E GARANTIA**

1.2.11.1. Os serviços devem fornecer atualizações que corrijam falhas de segurança por um período de 60 meses, renovável na forma da legislação vigente.
1.2.11.2. Os serviços devem fornecer canal digital, disponível a qualquer hora do dia, de domingo a sábado, para contato com suporte técnico.
1.2.11.3. Os serviços deverão garantir compatibilidade com versões de banco de dados que estejam dentro do ciclo de vida de suporte do Oracle Database.
1.2.11.4. Os serviços deverão apresentar possibilidade de atualização de versão sem perda de histórico ou de configuração existente.
1.2.11.5. Os serviços deverão permitir o acesso simultâneo de vários técnicos do contratante ao suporte técnico, atendendo às demandas individualmente.

**1.2.12. REQUISITOS TEMPORAIS**

1.2.12.1. Os serviços de suporte e atualização de versão serão prestados de acordo com o calendário ciclo de vida do suporte prestado à versão do Oracle Database.

## 2. JUSTIFICATIVA CONTENDO: NECESSIDADE DA AQUISIÇÃO, OBJETIVOS ESPERADOS E RESULTADOS QUE SE PRETENDE ALCANÇAR COM A AQUISIÇÃO:

### 2.1. NECESSIDADE DA AQUISIÇÃO

2.1.1. Busca-se, por meio da contratação, manter atualizadas as licenças de *Options* de segurança Oracle adquiridas por este TRE, mantendo conformidade com os normativos elencados a seguir, tratando da questão da segurança e da proteção da privacidade dos dados sob custódia do TRE-DF, no escopo de dados armazenados em bancos de dados Oracle:
2.1.1.1. **Lei nº 13.709/2018**: Lei Geral de Proteção de Dados (LGPD);
2.1.1.2. **Resolução CNJ nº 363/2021**: Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;
2.1.1.3. **Resolução TSE nº 23650/2021**: Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;
2.1.1.4. **Resolução nº 23.644/2021**: Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
2.1.2. Na motivação de conformidade aos normativos referenciados, a problemática da salvaguarda de direito à privacidade dos cidadãos e da reputação institucional subsidiada pela proteção dos ativos de informação passa a ter importância chave. A proteção cibernética passa pela necessidade-dever de prover mecanismos adequados de segurança para as instâncias de armazenamento para onde fluem os dados coletados e tratados nas mais diversas soluções corporativas hospedadas na infraestrutura dos tribunais eleitorais; em suma, segurança para os bancos de dados.

### 2.2. OBJETIVOS E RESULTADOS

2.2.1. O objeto desta contratação é composto por atualização e suporte de programas (*options* e *packs*) adquiridos que permitem o uso de recursos avançados de segurança para os dados armazenados no "*Oracle Database*".

2.2.2. O Oracle Database é um sistema de gerenciamento de banco de dados ao qual parte significativa das soluções da Justiça Eleitoral, cujas seminais datam de meados da década de 1990, é estruturalmente acoplada, gerando estreita dependência tecnológica das soluções ao produto. A adoção do Oracle Database tornou-se mandatória – como um padrão "de fato" – para os Tribunais Regionais Eleitorais, vez que devem consumir soluções providas, de modo compulsório e uniformizado, pelo Tribunal Superior Eleitoral e, de outro lado, necessitam prover soluções internas complementares às do TSE e, ainda, venham a ter pretensão de compartilhar estas soluções complementares com seus pares eleitorais. Consequentemente, o produto Oracle Database é mantido e utilizado neste TRE.

2.2.3. O Oracle Database fornece recursos elementares de segurança e auditoria para os seus bancos de dados. Entretanto, confrontado por um cenário de crescente ameaça aos ativos de informação, seja por ataques cibernéticos externos, seja por roubo ou extravio por pessoas acreditadas pela organização, e considerando os danos à imagem institucional e de responsabilização do órgãos em caso de extravio, roubo, divulgação ou sequestro destes ativos, estabeleceu-se outro patamar, mais elevado, de requisitos para aprimoramento dos mecanismos de segurança, resultando na necessidade de extensão dos recursos de proteção do Oracle Database.

2.2.4. A extensão dos recursos de proteção do produto Oracle Database se dá pela oferta de programas nativos e integrados com recursos sofisticados de segurança e privacidade dos ativos de informação, alguns dos quais disponibilizados automaticamente no momento de sua própria instalação. Entretanto, para que se faça uso dos recursos avançados de segurança e privacidade providos por estes programas ao produto Oracle Database, torna-se imperativo o licenciamento prévio, de caráter individualizado, do contrário, o utilizador dos programas incorrerá em ilegalidade decorrente de infrações contratuais sujeitas a penalidades.

2.2.5. Esses programas (*options*) permitem o aprimoramento da proteção de dados, do controle de acesso aos dados, da auditoria e do monitoramento dos ativos de informação, pilares da segurança e privacidade, visa a obter os resultados descritos a seguir na segurança dos bancos de dados Oracle.

2.2.6. Porém, devida a crescente evolução de ataque e descoberta de novas vulnerabilidades de forma constante, e para que esses programas (*options*) funcionem de forma efetiva, é necessário que estes se encontrem na última versão disponibilizada.

2.2.7. A contratação proposta da aquisição de atualização e suporte das *options* de segurança do banco de dados Oracle visa manter esses programas o mais atualizado possível, aumentando a proteção dos dados e mantendo o suporte para aprimoramento dessa proteção, além da correção de problemas e tratamento de incidentes mais complexos.

## 3. LISTA DOS ATOS NORMATIVOS PERTINENTES À AQUISIÇÃO, OS QUAIS DEVEM SER PREVIAMENTE ANALISADOS:

3.1. Lei de Licitações de Contratos - Lei nº 14.133/2021;
3.2. Resolução CNJ nº 468/2022 e anexos - disciplina as contratações de TIC no PJ;
3.3. Lei Geral de Proteção de Dados - Lei nº 13.709/2018;
3.4. Resolução CNJ nº 370/2021 - ENTIC-JUD 2021-2026 - disciplina a estratégia de TIC no PJ;
3.5. Resolução CNJ n° 396/2021 - ENSEC-PJ - disciplina a estratégia de Segurança Cibernética no PJ;
3.6. Resolução CNJ n° 290/2021 - protocolo de gerenciamento de crises cibernéticas no âmbito do PJ;
3.7. Resolução CNJ n° 292/2021, - protocolo de prevenção de incidentes cibernéticos no âmbito do P J;
3.8. Resolução TSE nº 23.664/2021 - Política de Segurança da Informação (PSI).

## 4. LEVANTAMENTO DE MERCADO (IDENTIFICAÇÃO DAS DIVERSAS SOLUÇÕES DISPONÍVEIS NO MERCADO E CONTRATAÇÕES SIMILARES REALIZADAS POR OUTROS ÓRGÃOS PÚBLICOS) E JUSTIFICATIVA PARA ESCOLHA DO OBJETO QUE SE ALMEJA CONTRATAR (RAZÃO DA ESCOLHA DA SOLUÇÃO EM CONTRATAÇÃO COM OUTRAS DISPONÍVEIS NO MERCADO):

4.1. Os produtos relativos a banco de dados Oracle são atendidos de forma exclusiva, em termos de atualização e suporte, pela Oracle do Brasil Sistemas Ltda, não existindo outros fornecedores no mercado para atender essa demanda de contratação, sendo realizado por empresa única, conforme declaração constante na certidão da Associação Brasileira das Empresas de Software (ABES) (id 1522467), anexada ao processo SEI onde se processa a contratação.

4.2. O levantamento de mercado realizado demonstra a inviabilidade de competição, a partir de outras contratações públicas que realizam contratação de mesma natureza por inexigibilidade, tais como TRE-PR (id 1523420), TRE-MA (id 1523430) e MP-SC (id 1523437) que se encontram anexados ao processo SEI 0008928-80.2023.6.07.8100.

4.3. Opta-se pela vigência inicial de 60 (sessenta meses), renováveis por mais um período de 60 meses (cf. art. 107 da Lei 14.133/2021). A essencialidade e necessidade da contratação do serviço de atualização e suporte para as licenças dos programas de segurança de uso do *Oracle Database Enterprise Edition* estender-se por mais de um exercício financeiro reside nos seguintes fatos:

4.3.1. As licenças já adquiridas por este tribunal são de natureza perpétua;

4.3.2. Existe a necessidade de manter a versão dos programas de segurança que compõem o sistema de Gerenciamento de Banco de dados sempre atualizadas para se usufruir das melhorias e/ou correção de defeitos, além da mitigação de vulnerabilidades que facilitariam a ataques externos à base;

4.3.3. Suporte e documentação adequada para tratar defeitos de natureza do hardware ou do software.

4.4. Tem também o objetivo de aproveitar melhor a ferramenta em virtude de a curva de aprendizagem ser grande, o que resulta em demora na aquisição dos conhecimentos e habilidades necessárias para operacionalizá-la de forma eficaz. Equipes que utilizam ferramentas desse porte demoram para ter maturidade na sua utilização.

4.5. A contratação plurianual se mostra maior economicidade para a organização tendo em vista:

4.5.1. De acordo com a referida política da Oracle do Brasil Ltda, a precificação da renovação de suporte técnico e atualização baseia-se no preço pago no momento de aquisição da solução de Software.

4.5.2. O percentual aplicado para um produto de Software específico representa, em média, 22% (vinte e dois por cento) dos valores de aquisição do Software;

4.5.3. O valor para contratação anual fica em R$ 144.915,65 (id 1591372), com possibilidade de correção a cada 12 meses pelo ICTI (Índice de Custos de Tecnologia da Informação, mantido pelo IPEA), se solicitado pela Contratada, e **pagamentos mensais**, conforme proposta da empresa. Outrossim, considerando os pagamentos para a vigência de 60 meses, o **valor na vigência total do Contrato é estimado em R$ 724.578,24** (setecentos e vinte e quatro mil quinhentos e setenta e oito reais e vinte e quatro centavos)**.**

| 2023/2024 | 2024/2025 | 2025/2026 | 2026/2027 | 2027/2028 | **Total** |
|---|---|---|---|---|---|
| **R$ 144.915,65** | **R$ 144.915,65** | **R$ 144.915,65** | **R$ 144.915,65** | **R$ 144.915,65** | **R$ 724.578.24** |

4.5.4. Algumas **considerações** acerca da solução pretendida, à luz da Resolução nº 468/2022:

4.5.4.1. ***Avaliação acerca do grau de dependência da solução a ser contratada e planejem ações, a fim de minimizar impactos causados por eventual necessidade de substituir a solução a ser adquirida (Acórdão 2.569/2018 Plenário)***: o Banco de Dados da Oracle é utilizado por toda a Justiça Eleitoral e abriga o Cadastro Nacional de Eleitores. A decisão de substituição desse ativo tecnológico não depende apenas do TRE-DF mas, principalmente do TSE, e somente ele é que pode criar a estratégia de migração para outra tecnologia. Dessa maneira, faz-se necessário a manutenção do suporte técnico e atualização da solução existente no Tribunal.

4.5.4.2. ***Avaliação acerca da relação custo-benefício de manter a solução implantada ou de substituí-la, em casos que, mesmo havendo alto impacto na migração da solução, haja ganhos financeiros para a organização (Acórdão 2.569/2018 Plenário)***: como abordado acima, a utilização do

Banco de Dados Oracle se insere na estratégia de toda a Justiça Eleitoral, e não cabe somente ao TRE-DF a decisão migrar a tecnologia para outra, ainda que os custos sejam menores. Dessa maneira, faz-se necessário a manutenção do suporte técnico e atualização da solução existente no Tribunal.

4.5.4.3. ***Avaliação acerca do custo/benefício de contratar os serviços de suporte técnico e de atualização de versões, sejam ambos ou somente um deles, ou de não contratar nenhum desses serviços, considerando elementos como a necessidade de negócio que motive a contratação desse serviço e o preço praticado por esse serviço, de acordo com a Constituição Federal, art. 37, caput (parágrafos 287 a 290 e 299 a 302) (Acórdão 2.569/2018 Plenário)***: a principal motivação de contratação de suporte técnico e atualização da versão é, justamente, o tema de fundo da demanda pretendida, qual seja, a proteção dos ativos informacionais que residem no Banco de Dados Oracle. De fato, a segurança cibernética passou a ser tema essencial ao Poder Judiciário, uma vez que um incidente cibernético pode ter consequências catastróficas às funções institucionais do Poder Judiciário e uma estratégia de proteção passou a ser primordial para evitar ou minimizar consequências de perda, furto/roubo de dados. O custo/benefício de uma ação preventiva de atualização de versão, adição de patches de segurança é um custo muito menor do que remediar após um incidente cibernético. Por outro lado, a atualização de versão, adição de patches de segurança e suporte técnico são realizados apenas pela empresa contratante, não havendo outra solução que contratá-la para esse fim.

## 5. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DO OBJETO, COM DEFINIÇÃO E DOCUMENTAÇÃO DO MÉTODO PARA AVALIAR SE O OBJETO É DIVISÍVEL, COM BASE NAS PARTICULARIDADES DO MERCADO FORNECEDOR (DEFINIÇÃO DO TIPO DE LICITAÇÃO/ADJUDICAÇÃO):

5.1. Pelo fato de os serviços contratados serem exclusivos da Oracle do Brasil Sistemas Ltda, decide-se pelo **não parcelamento do objeto**, uma vez que é tecnicamente inviável, e constitui-se uma solução única, que não pode ser dividida lógica ou fisicamente e é proveniente de um fornecedor exclusivo, nos termos do art. 40, V, "b" e §3º, II e III da Lei 14.133/2021.

5.2. Considerando a exclusividade do fornecedor da solução e a impossibilidade de divisão do objeto, e pelo fato de se tratar de contratação direta, não há adjudicação pois o ato de ratificação de dispensas e inexigibilidades produz efeitos equivalentes aos da homologação da licitação (cf. "*É necessária a adjudicação nos processos de contratação direta?*" in *Zênite Blog*, link em: https://zenite.blog.br/e-necessaria-a-adjudicacao-nos-processos-de-contratacao-direta/, visto em: 20/11/2023).

## 6. JUSTIFICATIVA PARA A NATUREZA DOS BENS OU SERVIÇOS: FORNECIMENTO OU SERVIÇOS; CONTÍNUOS OU NÃO; COMUNS OU NÃO; SOLUÇÃO DE TIC; ENGENHARIA – ESPECIFICAR SE SE TRATAR DE REFORMA DE EDIFÍCIO OU EQUIPAMENTO; TERCEIRIZAÇÃO COM CESSÃO EXCLUSIVA DE MÃO DE OBRA; SERVIÇOS OU FORNECIMENTO POR DEMANDA):

6.1. Trata-se de contratação com prestação de serviços de suporte técnico, atualização de versão, bem como de disponibilização de *patches* de segurança, o que em princípio teria vigência máxima de 60 meses, conforme o art. 106 da Lei nº 14.133/2021. No entanto, a contratação se reveste de requisitos de **essencialidade** e **continuidade**, uma vez que a segurança do banco de dados do TRE-DF é prioridade da Administração, bem como também do Poder Judiciário. Isso é verdade ao considerarmos que os requisitos de segurança da informação passou a ter imensa importância no âmbito da digitalização do PJ: o CNJ, por ocasião da ENTIC-JUD passou a adotar uma estratégia de Tecnologia da Informação, que rendeu frutos de agilidade e rapidez com sistemas informáticos que modernizaram a face do Judiciário. Estes sistemas disponibilizados aos cidadãos, advogados, juízes e promotores, tais como o PJe, fizeram uma profunda mudança na forma de se conduzir os processos judiciários, promover direitos e agilizar a prestação jurisdicional. Isso, porém, veio com o ônus de buscar a aplicação de instrumentos e técnicas de segurança cibernética. Assim, por isso, o CNJ criou, pela Resolução CNJ 396/2021, o ENSEC-PJ, ou seja, a Estratégia Nacional de Segurança Cibernética do PJ. Por ela, está descrito todas as ações necessárias aos Tribunais para assegurar a integridade de acesso e de dados, além de providências em caso de incidente cibernético. Por isso, as contratações no âmbito da Segurança da Informação passaram a ter prioridade, possuindo, até, rubrica de orçamento próprio.

6.2. No caso desta demanda, a segurança cibernética de Banco de Dados Oracle, utilizados pela Justiça Eleitoral, tem prioridade especial, uma vez que os dados essenciais deste Tribunal, estão guardados e organizados neste software. A essencialidade, em função do contexto, bem como da normativa própria direcionada a todo o Judiciário, implica que a contratação possui um caráter contínuo, sem sem ela, o mister institucional ficaria em perigo, principalmente nestes tempos de risco cibernético aumentado.

6.3. Por fim, a essencialidade, e, portanto, o caráter contínuo da contratação, se mostra preponderante no tempo, uma vez que, dentre os requisitos de segurança cibernética, a atualização e disponibilização de patches de segurança, os quais são distribuídos com o tempo e a descoberta de novas ameaças cibernéticas.

## 7. NO CASO DE SERVIÇOS, ESTES DEVEM SER DEFINIDOS E JUSTIFICADA SUA NATUREZA CONTINUADA, CASO ASSIM SEJA, DEMONSTRANDO QUE O OBJETO DO CONTRATO CONSISTE EM PRESTAÇÃO DE SERVIÇOS DE NATUREZA CONTINUADA:

7.1. Como dito acima, a contratação **possui natureza continuada**, em função da necessidade imperiosa da manutenção da segurança do Banco de Dados Oracle, o qual possui dados essenciais para o mister deste Tribunal.

7.2. O TCU, há muito, **recomendava** a implementação de políticas e recursos de segurança da informação, como bem retratado no Acórdão 2938/2010 - Plenário: "*ENUNCIADO: Em atenção ao disposto na Resolução CNJ 90/2009 (art. 10) , é recomendável à Administração dos órgãos do Poder Judiciário implementar processo de gestão de riscos de segurança da informação, a fim de, entre outros objetivos, avaliar regularmente a probabilidade e o impacto dos riscos identificados, utilizando métodos qualitativos e quantitativos, observando as práticas contidas no Cobit 4.1, PO9.4 - Avaliar e gerenciar riscos de TI e na NBR 27005 - Gestão de Riscos de Segurança da Informação*".

7.3. Na nova Lei de Licitações (Lei nº 14.133/2021), a natureza continuada é definida no art. 6º, XV: "*serviços e fornecimentos contínuos: serviços contratados e compras realizadas pela Administração Pública para a **manutenção da atividade administrativa, decorrentes de necessidades permanentes ou prolongadas***". Ou seja, a proteção cibernética do Banco de Dados Oracle é **necessidade de alta importância**, pois sem ela será impossível a manutenção da atividade administrativa e jurisdicional do TRE-DF, se houver incidente cibernético, que pode ser "*qualquer evento adverso, relacionado à segurança dos sistemas de computação ou das redes de computadores, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação*"( *in* site ANAC, visto em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/etir/o-que-e-um-incidente-de-seguranca-cibernetica).

7.4. Dessa maneira, a demanda se reveste de natureza continuada, sendo relevante informar que a Lei nº 14.133/2021, prevê em seus artigos 106 e 107 a possibilidade de estabelecer contratos com duração de 5 anos, bem como a possibilidade de prorrogar até o limite de 10 anos.

## 8. DURAÇÃO DO CONTRATO (VIGÊNCIA) E A POSSIBILIDADE DE PRORROGAÇÃO:

8.1. A duração do Contrato em relação à atual demanda é de 60 meses, renováveis por mais 60 meses, considerando o juízo de oportunidade e conveniência da Administração, nos termos do art. 107 da Lei nº 14.133/2021.

## 9. ESTIMATIVA DAS QUANTIDADES, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE LHE DÃO SUPORTE (DEFINIÇÃO E DOCUMENTAÇÃO DO MÉTODO UTILIZADO PARA REALIZAR A ESTIMATIVA DE QUANTIDADES, BEM COMO A RELAÇÃO ENTRE A DEMANDA E O QUANTITATIVO ESTIMADO):

**9.1. DOS QUANTITATIVOS**

9.1.1. Os quantitativos licenças estão dispostos na seguinte tabela:

| Item | Descrição do serviço | Unidade de medida | Quantidade |
|---|---|---|---|
| 1 | Oracle Advanced Security - Processor Perpetual - **Suporte Técnico** | Unidade | 4 |
| | Oracle Advanced Security - Processor Perpetual - **Atualização e Patches** | | |
| 2 | Oracle Database Vault - Processor Perpetual - **Suporte Técnico** | Unidade | 4 |
| | Oracle Database Vault - Processor Perpetual - **Atualização e Patches** | | |
| 3 | Oracle Data Masking and Subsetting Pack Processor Perpetual - **Suporte Técnico** | Unidade | 4 |
| | Oracle Data Masking and Subsetting Pack Processor Perpetual - **Atualização e Patches** | | |

9.1.2. Os quantitativos de serviços estão relacionados à quantidade de licenças de *Options* de Banco de Dados Oracle existentes neste Regional.

## 10. ESTIMATIVA DE PREÇOS, SEMPRE QUE POSSÍVEL NA FORMA DE COMPOSIÇÃO DE CUSTOS UNITÁRIOS, PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS OU INDICAÇÃO DE PREÇOS REFERENCIAIS, INCLUINDO NOS AUTOS OS DOCUMENTOS QUE LHE DÃO SUPORTE:

10.1. A estimativa de preços está de acordo com o valor atual orçado pela empresa, bem como os valores das contratações públicas pesquisadas, o qual constitui a tabela abaixo (custo unitário anual):

| Itens (conforme tabela do tópico 9.1.1) | Orçamento Oracle - valor anual por unidade (id 1591372) | TRE-MA valor anual por unidade - inexigibilidade 44/203 (id 1573160) | TRE-MA valor anual por unidade - Inexigibilidade 102/2023 (id 1573164) | TRE-GO valor anual por unidade - Contrato 55/2023 (id 1573165) | TRE-SP valor anual por unidade - Contrato 1/2024 (id 1573178) | TRE-ES valor anual por unidade - Contrato 36/2023 (id 1573168) | **Preço médio** |
|---|---|---|---|---|---|---|---|
| Oracle Advanced Security (4 un) | R$ 14.300,88 (un) | R$ 18.111,34 (un) | --- | R$ 12.078.12 (un) | R$ 11.220.46 (un) | R$ 13.244,93 (un) | R$ 13.791,15 |
| Oracle Database Vault (4 un) | R$ 10.964,02 (un) | --- | R$ 8.869,35 | R$ 9.259,89 (un) | R$ 8.602,35 (un) | R$ 10.154,43 (un) | R$ 9.570,01 |
| Oracle Data Masking and Subsetting Pack (4 un) | R$ 10.964,01 (un) | R$ 13.870,03 (un) | --- | R$ 9.259.9 (un) | R$ 8.602,34 (un) | R$ 10.154,43 (un) | R$ 10.570,14 |

10.2. Importante ressaltar que os valores da Proposta da Oracle são estimados, pois a depender do período que houver a contratação, haverá a aplicação da "*Reintatement Fee*", que é uma taxa aplicável a depender do interrégno de tempo entre o final e o início de novo período de do suporte técnico e atualização de software.

## 11. INDICAÇÃO, SALVO IMPOSSIBILIDADE DEVIDAMENTE JUSTIFICADA, DOS CRITÉRIOS E DAS PRÁTICAS DE SUSTENTABILIDADE, OS QUAIS DEVEM SER INCLUÍDOS NA ESPECIFICAÇÃO TÉCNICA DO OBJETO OU COMO OBRIGAÇÕES DA CONTRATADA:

11.1. Considerando que se trata de prestação de suporte técnico e atualização, em geral feito de modo remoto ou virtual, não há critérios e práticas de sustentabilidade aplicáveis.

## 12. IDENTIFICAÇÃO DA NECESSIDADE DE A FUTURA CONTRATADA PROMOVER A TRANSIÇÃO CONTRATUAL COM TRANSFERÊNCIA DE CONHECIMENTO, TECNOLOGIA E TÉCNICAS EMPREGADAS, SE APLICÁVEL:

12.1. Uma vez que se trata de prestação de suporte técnico e atualização, realizados pela própria empresa fornecedora do software, não há possibilidade de transição contratual e transferência de conhecimento/tecnologia que sejam aplicáveis.

## 13. INDICAÇÃO DAS PROVIDÊNCIAS NECESSÁRIAS PARA ADEQUAR O AMBIENTE DO TRIBUNAL À AQUISIÇÃO, O QUE É PAUTADO PELOS SEGUINTES CRITÉRIOS, COM ELABORAÇÃO DE CRONOGRAMA DE ATIVIDADES, SE NECESSÁRIO:

13.1. Não há necessidade de alteração da infraestrutura tecnológica, elétrica e física, nem necessidade de alteração em mobiliário, bem como impacto ambiental da implantação da solução demandada.

## 14. INDICAÇÃO DA NECESSIDADE DE REALIZAR NOVAS CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES OU DA NECESSIDADE DE RELACIONAR A CONTRATAÇÃO COM OUTRAS JÁ EXISTENTES:

14.1. Não há contratações correlatas ou interdependentes a serem realizadas em conjunto com a presente demanda.

## 15. A DEPENDER DO OBJETO, VERIFICAR A EXISTÊNCIA DE INTENÇÃO DE REGISTRO DE PREÇOS (IRP) DIVULGADA OU ATA DE REGISTRO DE PREÇOS (ARP) VIGENTE DE OUTRO ÓRGÃO FEDERAL E SE A PARTICIPAÇÃO OU ADESÃO DO TRE-DF SERIA TECNICAMENTE ADEQUADA E ECONOMICAMENTE VANTAJOSA:

15.1. Não há IRP ou ARP vigente aplicáveis a esta demanda.

## 16. A CLASSIFICAÇÃO ORÇAMENTÁRIA COM A INDICAÇÃO DA FONTE DE RECURSO DO ORÇAMENTO DO ÓRGÃO PREVISTO PARA ATENDER A NECESSIDADE DA CONTRATAÇÃO (SE NECESSÁRIO, A EQUIPE DEVERÁ DILIGENCIAR À SEPEO PARA ESCLARECIMENTOS):

16.1. Segundo informações da SEPEO, a presente demanda classifica-se na Ação 21EE: PO SEG0 - Segurança da Informação, na natureza de despesa 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - PJ, no subitem 07 - Manutenção Corretiva / Adaptativa e Sustentação de Softwares, com valores complementares remanejados da Ação 20GP, elemento de despesa 33.90.40 (Serviços de Tecnologia da Informação e Comunicação, subitem 12).

## 17. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

17.1. A Equipe de Planejamento da Contratação, com fundamento na Resolução CNJ nº 468/2022, e após concluir os estudos técnicos preliminares aqui apresentados, declara ser viável a contratação pretendida.

| EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO | | |
|---|---|---|
| **Integrante Demandante** | **Integrante Técnico** | **Integrante Administrativo** |
| Diego Batista Assunção do Vale<br>Matrícula: 1971 | Leandro Amorim Carisio<br>Matrícula: 2131 | Rafael Dittberner<br>Matrícula: 0562 |

Documento assinado eletronicamente por **LEANDRO AMORIM CARISIO**, **Chefe de Seção**, em 09/04/2024, às 12:26, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RAFAEL DITTBERNER**, **Coordenador**, em 09/04/2024, às 16:51, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIEGO BATISTA ASSUNÇÃO DO VALE**, **Técnico Judiciário**, em 09/04/2024, às 16:54, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-df.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1590046** e o código CRC **407106B3**.