



TRIBUNAL REGIONAL ELEITORAL DO DF  
Praça Municipal Qd. 02, Lote 06 - Bairro Plano Piloto - CEP 70094-901 - Brasília - DF

## TERMO DE REFERÊNCIA

(CONFORME RESOLUÇÃO CNJ Nº 468/2022)

### CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO (STIC)

#### 1. DEFINIÇÃO DO OBJETO E REQUISITOS TÉCNICOS:

##### 1.1. DEFINIÇÃO E DESCRIÇÃO DA SOLUÇÃO

1.1.1. O presente Termo de Referência visa trazer as especificações técnicas e condições administrativas da contratação de empresa para a prestação de 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 no 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		

1.1.4. Ressalte-se que a presente demanda de contratação faz parte do esforço de proteção de dados constantes do Banco de Dados Oracle e faz parte, também, da política de Cibersegurança do Tribunal contratante.

#### 1.2. REQUISITOS TÉCNICOS 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 suporte técnico, distribuição de patches de segurança e atualização de versão dos options *Oracle Advanced Security, Oracle Database Vault e Oracle Data Masking and Subsetting Pack*, por 60 meses.

1.2.2.2. A empresa contratada deve prestar 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:** 0 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. 0 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.

### 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 \(tre-df.jus.br\)](http://governanca.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. A contratada deverá fornecer credenciais seguras para a contratante a fim de acessar o suporte técnico e as atualizações de versão.

1.2.3.4. A contratante poderá alterar a senha de acesso ao suporte técnico e às atualizações sempre que considerar conveniente, sem necessidade de anuência da contratada.

1.2.3.5. A contratada não poderá 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**, constante do **Anexo II**.

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**, constante no Anexo II ao Termo de Referência, bem como assinar **Termo de Ciência da Política de Acesso aos Recursos de TIC e da Política de Gerenciamento de Crises Cibernéticas do TRE-DF**, constante no **Anexo III**.

### 1.2.4. REQUISITOS TECNOLÓGICOS E DE ARQUITETURA

1.2.4.1. 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. 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. Fornecer as credenciais de acesso ao Portal MY ORACLE SUPPORT.

1.2.4.4. 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. 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. A solução, quando composta de mais de um módulo ou programa/produto, deverá manter a compatibilidade entre os componentes, garantindo o funcionamento consistente e harmonioso.

1.2.4.7. Os serviços deverão manter a compatibilidade da solução com arquitetura *multi-tenant* e, também, para com a arquitetura *non-cdb* do Oracle Database.

## 1.2.5. REQUISITOS LEGAIS

1.2.5.1. Os serviços deverão manter a solução alinhada com os normativos elencados na seção “Fundamentação Legal” e as boas práticas das “Referências Técnicas” consideradas para a presente contratação.

1.2.5.2. Os serviços manterão a solução capaz de proteger dados de acessos não autorizados (Art. 6º, VII e Art. 46 da LGPD; CNJ nº 363/2021; Res. TSE nº 23.650/2021 e nº 23.644/2021).

1.2.5.3. Os serviços manterão a solução capaz de proteger dados de situações acidentais de destruição, perda, alteração, comunicação ou difusão (Art. 6º, VI e Art. 46, I, da LGPD).

1.2.5.4. Os serviços manterão a solução capaz de prevenir ocorrência de danos em virtude do tratamento de dados (Art. 6º, VIII da LGPD).

1.2.5.5. Os serviços manterão a solução capaz de comprovar a observância e o cumprimento de normas de proteção de dados (Art. 6º, X da LGPD; Res. TSE nº 23.650/2021).

1.2.5.6. Os serviços manterão a solução capaz de tornar os dados pessoais anônimos de modo não reversível (Art. 12, § 3º e Art. 16, II e IV, da LGPD).

1.2.5.7. Os serviços manterão a solução capaz de manter registro de auditoria das operações de tratamento de dados (LGPD, Art. 37, II e IV; Res. TSE nº 23.650/2021).

1.2.5.8. Os serviços manterão a solução capaz de informar 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).

1.2.5.9. Os serviços manterão a solução capaz de manter registro de auditoria de tentativa de violação ou violação de política de segurança (LGPD, Art. 48, III).

1.2.5.10. Os serviços manterão a solução capaz de permitir adoção de medidas técnicas para tornar os dados ininteligíveis para terceiros não autorizados a acessá-los (LGPD, Art. 48, § 3º; TSE nº 23.650/2021, Art. 14, IV).

1.2.5.11. Os serviços manterão a solução capaz de permitir medidas tais como a aposição de tarjas sobre dados pessoais ou a supressão parcial de números cadastrais (TSE nº 23.650/2021, Art. 7º, Parágrafo Único).

1.2.5.12. Os serviços manterão a solução capaz de permitir o uso de recursos criptográficos sobre os bancos de dados (Resolução nº 23.644/2021, Art. 9º, II e Art. 17).

1.2.5.13. 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 nº 9.279/1996 e Lei nº 9.609/1998).

## 1.2.6. REQUISITOS FUNCIONAIS

### 1.2.6.1. Criptografia de dados:

1.2.6.1.1. Os serviços manterão a solução capaz de realizar criptografia de dados na camada de armazenamento, de forma nativa e sem necessidade de utilização 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 manterão a solução capaz de apresentar os 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 manterão a solução capaz de permitir 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 manterão a solução capaz de permitir 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 manterão a solução capaz de permitir 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 manterão a solução capaz de utilizar chaves criptográficas armazenadas no Oracle wallet, nos padrões PKCS#12 e PKCS#5.

- 1.2.6.1.7. Os serviços manterão a solução capaz de incapacitar a leitura de dados 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 manterão a solução capaz de 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 manterão a solução capaz de 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 manterão a solução capaz de ser completamente integrada ao Oracle Database, com suporte à aceleração de criptografia baseada em hardware, compatível com tecnologia Intel® Advanced Encryption Standard Instruction (AES-NI).
- 1.2.6.1.11. Os serviços manterão a solução capaz de 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 manterão a solução capaz de utilizar de chaves de criptografia de padrões PKCS#12 e PKCS#5.
- 1.2.6.1.13. Os serviços manterão a solução capaz de permitir a compressão de dados em dados criptografados.
- 1.2.6.1.14. Os serviços manterão a solução capaz de não impedir o uso de *transportable tablespace* para dados criptografados.
- 1.2.6.1.15. Os serviços manterão a solução sem limitações quanto ao tipo e quanto ao tamanho do dado a ser criptografado.
- 1.2.6.1.16. Os serviços manterão 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 manterão a solução capaz de realizar, 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 manterão a solução 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 manterão 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 manterão a solução capaz de reescrever o dado consultado em tempo de execução.
- 1.2.6.2.6. Os serviços manterão 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 manterão 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 manterão 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 manterão 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 manterão a solução capaz de permitir o mascaramento e a produção de amostras quando em uso da ferramenta Oracle Database - Data Pump.

1.2.6.3.5. Os serviços manterão 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 manterão 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 manterão 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 manterão 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 manterão a solução capaz de ser integrada ao Oracle Database, sem a necessidade de uso de ferramentas de terceiros.

1.2.6.3.10. Os serviços manterão 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 manterão 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 manterão 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 manterão 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 manterão 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 manterão 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 manterão 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 manterão 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 manterão a solução 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 manterão 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 manterão 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 manterão 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 indicar 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 manterão a solução capaz se conformar ao ambiente tecnológico e físico que está em operação no contratante.

1.2.8.2. Os serviços manterão a solução capaz de atuar na camada de banco de dados sem comprometer o desempenho dos bancos de dados da contratante.

1.2.8.3. 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 poderão alterar 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 devem 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 devem manter a possibilidade de atualização de versão sem perda de histórico ou de configuração existente.

1.2.11.5. Os serviços devem manter a permissão do acesso simultâneo de vários técnicos do contratante ao suporte técnico, atendendo às demandas individualmente.

### 1.2.12. REQUISITOS TEMPORAIS

1.2.12.1. A solução deverá garantir o suporte e atualização de versão de acordo com o calendário ciclo de vida do suporte prestado à versão do Oracle Database.

## 2. FUNDAMENTAÇÃO DA CONTRATAÇÃO:

### 2.1. MOTIVAÇÃO DA CONTRATAÇÃO:

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 23.650/2021: 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 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.

2.1.3. Pode-se concluir que a contratação do serviço possui um aspecto essencial, uma vez que a privacidade e a segurança dos dados de cidadãos e dos vários processos judiciais e administrativos passaram a ter relevância dentro do dia-a-dia do Judiciário, e constitui uma forma de proteção da missão institucional do Tribunal.

2.1.4. O Oracle Database é um sistema de gerenciamento de banco de dados, ao qual parte significativa das soluções da Justiça Eleitoral, cujos inícios 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.

2.1.5. 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 dos 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.

2.1.6. 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.

2.1.7. Esses programas (*options*) adquiridos 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 dos bancos de dados Oracle.

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

2.1.9. 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, correção de problemas e tratamento de incidentes mais complexos.

## 2.2. OBJETIVOS A SEREM ALCANÇADOS:

### 2.2.1. Objetivo Geral:

2.2.1.1. O objetivo geral da contratação é a manutenção e proteção das funções institucionais deste Regional, que hoje conta com a tecnologia do Banco de Dados Oracle, o qual abriga dados de cidadãos, de processos judiciais e administrativos, bem como outros dados sensíveis, os quais são essenciais para o mister do TRE/DF.

### 2.2.2. Objetivos Específicos:

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

2.2.2.2. Além do mais, objetiva-se a disponibilização de *patches* de segurança, os quais visam eliminar ou mitigar as vulnerabilidades do software, quando conhecidas.

## 2.3. BENEFÍCIOS

2.3.1. Dentre os benefícios da contratação, encontra-se a dilação, no tempo, das garantias de segurança do Banco de Dados Oracle, que preliminarmente se estendem a 60 meses, renováveis por mais 60 meses, a critério da Administração.

2.3.2. Além do mais, a disponibilização do serviço é feita pela própria empresa fabricante/desenvolvedora da solução, o que garante que as correções de segurança e a atualização do sistema seja feita pelas melhores práticas do mercado, com segurança e integridade que pode ser exigida de quem idealizou o software.

## 2.4. ALINHAMENTO ESTRATÉGICO:

2.4.1. A contratação está em consonância com:

2.4.1.1. **PLANEJAMENTO ESTRATÉGICO DO PODER JUDICIÁRIO:** Dentre os objetivos da Resolução 325/2020 CNJ, pode-se destacar os seguintes Macrodesafios:

2.4.1.1.1. Perspectiva Processos Internos: APERFEIÇOAMENTO DA GESTÃO ADMINISTRATIVA E DA GOVERNANÇA JUDICIÁRIA;

2.4.1.1.2. Perspectiva Aprendizado e Crescimento: FORTALECIMENTO DA ESTRATÉGIA NACIONAL DE TIC E DE PROTEÇÃO DE DADOS.

2.4.1.2. **PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL DO TRE-DF (PEI):** De acordo com o Planejamento Estratégico do TRE-DF 2021/2026, nos termos da Resolução nº 7874/2021, observa-se a aderência às seguintes diretrizes:

2.4.1.2.1. **Missão:** Garantir a legitimidade do processo eleitoral.

2.4.1.2.2. **Visão:** Ser modelo de excelência na gestão do processo eleitoral, fortalecendo a credibilidade da Justiça Eleitoral perante a sociedade.

2.4.1.2.3. **Macrodesafios:**

2.4.1.2.3.1. Processos Internos: APERFEIÇOAMENTO DA GESTÃO ADMINISTRATIVA E DA GOVERNANÇA JUDICIÁRIA.

2.4.1.2.3.2. Aprendizado e Crescimento: FORTALECIMENTO DA ESTRATÉGIA NACIONAL DE TIC E DE PROTEÇÃO DE DADOS.

2.4.1.2.4. Indicadores:

2.4.1.2.4.1. INDICADOR 23: Índice de Governança de Tecnologia da Informação.

2.4.1.3. **PLANEJAMENTO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO 2023-2024 (PETIC):**

2.4.1.3.1. Perspectiva Processos Internos: Aprimorar a Segurança da Informação e Gestão de Dados.

2.4.1.3.2. Macrodesafio PEI-TRE-DF: IX - Fortalecimento da estratégia nacional de TIC e de proteção de dados.

2.4.1.3.3. Grupo 3 - Segurança da Informação e Proteção de dados: PTE-11 - Aperfeiçoar as estruturas de segurança da informação.

2.4.1.4. **Não se aplicam:** PLANO DE GESTÃO DO TRE-DF e PLANO DE OBRAS DO TRE-DF.

## 2.5. ESTUDOS PRELIMINARES:

2.5.1. Em atendimento à Resolução CNJ nº 468/2022, os Estudos Técnicos Preliminares sobre a presente aquisição foram realizados e podem ser consultados no SEI- id 1590107.

## 2.6. RELAÇÃO ENTRE A DEMANDA PREVISTA E QUANTIDADE DE BENS/SERVIÇOS:

2.6.1. A quantidade de serviços a serem contratados está relacionada à quantidade de licenças do Banco de Dados Oracle (quatro licenças de Banco de Dados Oracle) e está indicada no item 1.1.3.

2.6.2. Cada item refere-se a um serviço relacionado à uma determinada licença.

## 2.7. 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 :

2.7.1. 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) (doc nº 1522467), anexada ao processo SEI de contratação.

2.7.2. 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-MA (ids 1573160 e 1573164), TRE-GO (id 1573165), TRE-ES (id 1573168) e TRE-SP (id 1573178) que se encontram anexados ao processo SEI 0008928-80.2023.6.07.8100.

2.7.3. A Equipe de Planejamento opta pela vigência inicial de 60 (sessenta) meses, para uma melhor racionalização da utilização dos recursos humanos e financeiros, com a otimização sistemática dos processos de trabalho e redução dos custos processuais para renovação de contrato, em comparativo com a utilização de 12 meses, somado ao fato de que a demanda se reveste de natureza continuada, de modo que a Lei nº 14.133/2021, em seus artigos 106 e 107, prevê a possibilidade de estabelecer contratos com duração de 5 anos, bem como a possibilidade de prorrogá-los até o limite de 10 anos. Importante ressaltar, em acréscimo, que o serviço de atualização e suporte para as licenças dos programas de segurança de uso do Oracle Database Enterprise Edition estendem-se por mais de um exercício financeiro devido aos seguintes fatos:

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

2.7.3.2. 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;

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

2.7.4. Há, 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.

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

2.7.5.1. 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.

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

2.7.5.3. O valor para **contratação anual fica em R\$ 144.915,65** (cento e quarenta e quatro mil novecentos e quinze reais e sessenta e cinco centavos), 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 estimados em R\$ 12.076,30 (doze mil setenta e seis reais e trinta centavos)**, 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

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

2.7.5.4.1. **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.

2.7.5.4.2. **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.

2.7.5.4.3. **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.

## 2.8. PREÇOS E ADEQUABILIDADE ÀS CONDIÇÕES DE MERCADO:

2.8.1. Verifica-se, pela tabela abaixo, que os preços praticados pela empresa estão de acordo com o mercado. Os valores possuem ampla variação uma vez que cada órgão possui uma versão específica das licenças/software do Banco de Dados, bem como os serviços/software acessórios. De mais a mais, os valores são variáveis também se consideramos as diferentes infraestruturas dos órgãos pesquisados. Buscou-se aproximar das contratações que mais se assemelham às necessidades deste Regional. Como a Oracle do Brasil é a **única prestadora de serviços no país**, as variações dos preços públicos alcançados não seguem outro padrão



a não ser da avaliação da empresa. Abaixo os preços pesquisados de contratações atuais compatíveis com a pretendida:

Itens (conforme tabela do tópico 1.1.3.)	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

2.8.2. Considerando os preços ofertados na Proposta do id 1591372, verifica-se que estão **compatíveis com o mercado**.

## 2.9. ADEQUAÇÃO AO DECRETO 7.174/2010

2.9.1. Não se aplica as regras de preferência dispostas no art. 3º c/c 16-A da Lei nº 8.248, de 23 de outubro de 1991, e no art. 6º do Decreto no 7.174, de 12 de maio de 2010, por se tratar de contratação mediante inexigibilidade de licitação.

### 3. NATUREZA DO OBJETO:

3.1. 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 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 judiciais, 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**.

3.2. 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 ela, o mister institucional ficaria em perigo, principalmente nestes tempos de risco cibernético aumentado**.

3.3. 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.

3.4. 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.

3.5. 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*".

3.6. 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 ele 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/acao-a-informacao/seguranca-da-informacao/etir/o-que-e-um-incidente-de-seguranca-cibernetica>).

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

### 4. PARCELAMENTO DO OBJETO:

4.1. 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 oferecida pela empresa**, além de ser proveniente de um **fornecedor exclusivo**, nos termos do art. 40, V, "b" e §3º, II e III da Lei 14.133/2021.

4.2. 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).

## 5. **FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR:**

5.1. A contratação pretendida será realizada diretamente, por inexigibilidade de licitação, com fundamento no inciso I do caput do artigo 74 da Lei nº 14.133/2021.

5.2 Foi observado que a **Oracle do Brasil Sistemas Ltda** – CNPJ nº 59.456.277/0001-76, é a única empresa autorizada à execução do objeto da contratação, no âmbito do território nacional, estando esta exclusividade comprovada por meio das CERTIDÕES Nº 230912/40.585 e Nº 240130/41.215, expedidas pela Associação Brasileira das Empresas de Software – ABES (ids 1522467 e 1579007). A certificada e patente exclusividade da prestação dos serviços objeto deste TR, que culmina na inviabilidade de competição, é um dos fatores determinantes para persistir na presente contratação por intermédio de inexigibilidade de licitação, sendo a única opção para esta Administração.

5.3 As hipóteses de contratação direta por inexigibilidade de licitação, elencadas no artigo 74 da Lei nº 14.133/2021, somente se justificam quando se configura a inviabilidade de competição, diante da existência de apenas um objeto ou pessoa capaz de atender às necessidades da Administração Pública. Deste modo, restando caracterizada a exclusividade da empresa **Oracle do Brasil Sistemas Ltda** na "*prestação de serviço de suporte técnico e atualização de ferramentas opcionais de software de segurança para bancos de dados Oracle (options e packs)*", configura-se as condições para que ocorra a inexigibilidade de licitação, com fundamento no inciso I do caput do artigo 74 da Lei nº 14.133/2021.

### 5.4 Critérios de Habilitação Jurídica e qualificação técnica e econômico-financeira:

5.4.1 A Habilitação Jurídica e as Regularidades Jurídica, Fiscal e Econômico-Financeira serão exigidas de acordo com os arts. 68 e 69 da Lei nº 14.133/2021 e legislação correlata, como condição prévia para celebração do contrato, observada a estrutura jurídica da proponente, podendo ser comprovados por meio de consulta ao SICAF, preferencialmente.

5.4.2 Não será exigida a apresentação de atestado de capacidade técnica.

## 6. **INFORMAÇÕES ACERCA DO IMPACTO AMBIENTAL:**

6.1. Por se tratar de contratação de serviços de atualização de software, suporte técnico e segurança da informação, não há impacto ambiental mensurável e aparente.

## 7. **OBRIGAÇÕES**

### 7.1. **OBRIGAÇÕES DO CONTRATANTE**

7.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Demandante do contrato para acompanhar e fiscalizar a execução dos contratos;

7.1.2. Encaminhar formalmente a demanda para a contratada por meio de chamado técnico;

7.1.3. Aplicar à contratada, se necessário, as sanções administrativas regulamentares e contratuais cabíveis, garantida a ampla defesa e o contraditório.

7.1.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em Contrato;

7.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento dos serviços contratados;

7.1.6. Verificar a regularidade da situação fiscal da Contratada antes de efetuar o pagamento devido;

7.1.7. Notificar a CONTRATADA quanto a defeitos ou irregularidades verificadas na execução das atividades objeto deste Termo de referência, bem como, quanto a qualquer ocorrência relativa ao comportamento de seus representantes, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o TRE-DF;

7.1.8. Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução das atividades, assinando prazo para as correções que se fizerem necessárias.

### 7.2. **OBRIGAÇÕES DA CONTRATADA**

7.2.1. A CONTRATADA deverá disponibilizar ao TRE-DF, as atualizações, correções, alertas de segurança e novas versões dos produtos contratados durante o prazo de vigência do contrato;

7.2.2. Os manuais dos softwares provenientes da atualização dos Bancos de Dados Oracle, deverão ser disponibilizados, sempre que forem lançadas novas versões, sem ônus adicional para o TRE-DF;

7.2.3. Disponibilização de um **canal direto** com a CONTRATADA, podendo ser classificada em dois níveis (atualização de versões e suporte técnico), sendo:

7.2.3.1. **Atualização de versões:** compreende o fornecimento de correções, atualizações críticas, novas versões do produto, alertas de segurança que forem disponibilizadas pela CONTRATADA, provendo a garantia de evolução tecnológica e funcionamento adequado do produto;

7.2.3.2. **Suporte técnico:** representa a disponibilização de uma infraestrutura de atendimento, por telefone ou via portal de internet do fabricante.

7.2.4. O serviço de suporte técnico envolverá as atividades necessárias, para garantir a operação contínua dos softwares componentes da solução. Desta forma, farão parte do escopo das atividades de suporte:

7.2.4.1. Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades relacionadas a cada software componente da solução;

7.2.4.2. Resolução de problemas que limitem ou impeçam o desenvolvimento e/ou execução das aplicações do TRE-DF, que façam uso efetivo das funcionalidades dos softwares que compõem a solução.

7.2.5. O serviço de atendimento telefônico deverá ser prestado em idioma português do Brasil;

7.2.6. O serviço de suporte técnico deverá estar disponível para abertura e acompanhamento de chamados em tempo integral (24 horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados), em ambas as modalidades;

7.2.7. Deverá ser disponibilizada uma ferramenta de pesquisa em base de conhecimento de solução de problemas e documentos técnicos do fabricante;

7.2.8. O TRE-DF poderá efetuar um número ilimitado de chamados de suporte durante a vigência do contrato para suprir suas necessidades de utilização dos produtos contratados;

7.2.9. Deverá ser fornecido ao TRE-DF, um número de telefone que possibilite ligações gratuitas para a central de suporte técnico do fabricante do produto (tipo 0800), ou com custo de ligação local, para fins de abertura e acompanhamento de chamados;

7.2.10. Deverá ser fornecido um conjunto de identificadores e respectivas senhas de acesso para pessoas autorizadas a abrir e acompanhar os chamados de suporte;

7.2.11. Ao final da abertura de cada atendimento, deverá ser disponibilizado um registro do chamado técnico contendo no mínimo:

7.2.11.1. Número do chamado;

7.2.11.2. Data e hora do chamado;

7.2.11.3. Severidade do erro;

7.2.11.4. Previsão de atendimento.

7.2.12. Ao abrir um chamado, o TRE-DF poderá classificá-lo em 4 (quatro) níveis de severidade:

7.2.12.1. **Severidade 1** - O uso em produção dos aplicativos é paralisado ou está severamente impactado de tal forma, que é impossível continuar trabalhando de forma razoável. A operação passa a ser crítica para o negócio e a situação constitui uma emergência. Um problema severidade 1 pode possuir uma ou mais das seguintes características: informação corrompida; uma função crítica documentada não está disponível; o aplicativo se desliga, causando demoras inaceitáveis ou indefinidas para recursos ou respostas; o aplicativo falha repetidamente, após tentativas de reinicialização;

7.2.12.2. **Severidade 2** - O problema causa uma grave perda de funcionalidade. Não está disponível nenhuma alternativa ou processo alternativo, no entanto, a operação pode continuar de modo restrito;

7.2.12.3. **Severidade 3** - O problema causa uma pequena perda do serviço. O impacto é uma inconveniência, a qual pode exigir uma alternativa ou um processo alternativo para restaurar as funcionalidades;

7.2.12.4. **Severidade 4** - O problema não causa nenhuma perda de funcionalidade. O eventual resultado não impede a operação dos sistemas. Os chamados podem tratar de requisição de informações, melhorias ou esclarecimentos relativos à documentação sem impacto na operação do aplicativo.

7.2.13. O horário de atendimento de chamado classificado como de severidade 1, será em tempo integral (24 horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados);

7.2.14. O horário de atendimento de chamados classificados como de severidade 2 será de segunda a sexta das 6h às 24h e sábado das 8h às 20h;

7.2.15. O horário de atendimento de chamados classificados como de severidade 3 será de segunda a sexta das 8h às 20h e sábado das 8h às 12h;

7.2.16. O horário de atendimento de chamados classificados como de severidade 4 será de segunda a sexta das 8h às 20h;

7.2.17. Ao final de cada atendimento a CONTRATADA deverá disponibilizar **laudo técnico** contendo no mínimo:

7.2.17.1. Número do chamado;

7.2.17.2. Data e hora do chamado;

7.2.17.3. Data e hora do início e do término do atendimento;

7.2.17.4. Severidade do erro;

7.2.17.5. Identificação do problema;

7.2.17.6. Solução aplicada;

7.2.18. A finalização de cada atendimento, só poderá ser efetuada com a anuência do responsável técnico do TRE-DF.

7.2.19. A Contratada deverá devolver valores eventualmente recebidos antecipadamente, referentes aos serviços objetos deste TR ainda não executados, em hipótese de inexecução contratual prevista no Contrato.

### 7.3. DO INSTRUMENTO DE MEDIÇÃO DE RESULTADO (IMR)

#### 7.3.1. INFORMAÇÕES GERAIS

7.3.1.1. O Instrumento de Medição de Resultado – IMR é o ajuste entre o provedor de serviços e o órgão contratante, que define, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento.

7.3.1.2. Objetivo a atingir: Prestação do serviço em elevados níveis de qualidade.

7.3.1.3. Forma de avaliação: Definição de situações que caracterizem o não atingimento do objetivo, e atribuição de descontos no valor de pagamento devido.

7.3.1.4. Sanções: embora a aplicação de índices de desconto seja instrumento de gestão contratual, não configurando sanção, a Contratante poderá, pela qualidade insuficiente, aplicar as penalidades previstas em contrato.

### 7.3.2. CONDIÇÕES GERAIS

7.3.2.1. Para o acompanhamento e avaliação dos serviços da Contratada será estabelecido e utilizado o Instrumento de Medição de Resultado – IMR entre as partes, baseando-se em indicadores e metas definidos neste documento.

7.3.2.2. A análise dos resultados destas avaliações pela Contratante poderá resultar em penalidades, nos termos do Item 8.6 deste TR, caso a Contratada não cumpra com os seus compromissos de apresentação, pontualidade, disponibilidade e de prestação do objeto contratual, conforme estabelecido pelos indicadores.

7.3.2.3. O IMR deve ser considerado e entendido pela Contratada como um compromisso de qualidade que assumirá junto à Contratante. O IMR é um instrumento ágil e objetivo de avaliação da qualidade da execução contratual, associando o pagamento à qualidade efetivamente obtida.

7.3.2.4. Para o recebimento integral do valor contratado, a empresa contratada deverá cumprir com suas obrigações contratuais, em especial as dispostas nos indicadores de desempenho.

7.3.2.5. O IMR será implementado a partir da primeira medição da data de assinatura do contrato, cabendo ao Fiscal Técnico do contrato avaliar frequentemente a execução dos serviços prestados.

### 7.3.3. PONTUAÇÃO E APLICAÇÃO DO IMR

ITEM A SER AVALIADO	PONTUAÇÃO	PESO
Chamado Severidade 1	0 - 5	10
Chamado Severidade 2	0 - 5	6
Chamado Severidade 3	0 - 5	3
Chamado Severidade 4	0 - 5	1
Laudo Técnico	0 - 5	1

7.3.3.1. A forma de cálculo é que gerará a glosa no pagamento mensal é a seguinte:

$$\text{Valor\_Item} = \text{PONTUAÇÃO} \times \text{PESO}$$

$$\text{Avaliação\_Mensal}_{\text{mês}} = (\text{Valor\_Item}_1 + \text{Valor\_Item}_2 + \dots + \text{Valor\_Item}_n) / n_{\text{ITENS\_AVALIADOS}}$$

7.3.3.2. Tabela de Glosa no Pagamento Mensal:

Avaliação_Mensal <sub>mês</sub>	% de glosa no pagamento mensal
40 - 50	5% (ou 0,05)
30 - 39	4% (ou 0,04)
20 - 29	1% (0,01)
10 - 19	0,5% (0,005)
1 - 9	0,1% (ou 0,001)

7.3.3.3. Assim, o pagamento mensal será calculado da seguinte maneira:

$$\text{Pagamento}_{\text{mês}} = (1 - \text{Glosa}_{\text{mês}}) \times \text{Pagamento}_{\text{contrato}}$$

Onde: Pagamento<sub>mês</sub> = Pagamento com IMR aplicado no mês; Glosa<sub>mês</sub> = Porcentagem de Glosa no mês, conforme a tabela do item 7.3.3.2.; Pagamento<sub>contrato</sub> = Pagamento mensal estipulado no contrato

## 8. MODELO DE GESTÃO E EXECUÇÃO DO CONTRATO

### 8.1. FORMA DE SOLICITAÇÃO

8.1.1. Todas as solicitações serão feitas por meio do encaminhamento da Ordem de Fornecimento de Serviço, através de plataforma web, correio eletrônico (e-mail), serviço telefônico e/ou aplicativo de mensagens instantâneas (WhatsApp, Telegram e semelhantes).

### 8.2. ROTINAS DE EXECUÇÃO:

8.2.1. A CONTRATADA deverá disponibilizar ao TRE-DF as atualizações críticas, correções, alertas de segurança e novas versões dos produtos contratados durante o prazo de vigência do contrato;

8.2.2. Os manuais dos softwares componentes da solução, deverão ser atualizados, sempre que forem lançadas novas versões, sem ônus adicional para o TRE-DF;

8.2.3. Disponibilização de um **canal direto** com o fabricante, podendo ser classificada em dois níveis (atualização de versões e suporte técnico), conforme o item 7.2.3;

8.2.4. O serviço de **suporte técnico** envolverá as atividades necessárias, para garantir a operação contínua dos softwares componentes da solução, conforme o item 7.2.4;

8.2.5. O serviço de suporte técnico deverá estar disponível para abertura e acompanhamento de chamados em tempo integral (24 horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados), em ambas as modalidades;

8.2.6. Ao final de cada atendimento a CONTRATADA deverá disponibilizar **laudo técnico**, conforme o item 7.2.17.

### 8.3. MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA:

#### 8.3.1. A CONTRATADA deverá:

8.3.1.1. manter **sigilo**, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto identificado como confidencial no momento de sua divulgação que tomar conhecimento em razão da execução do presente contrato, devendo orientar seus empregados nesse sentido;

8.3.1.2. manter em **caráter confidencial** as informações relativas:

- 8.3.1.2.1. à política de segurança adotada pelo CONTRATANTE e as configurações de hardware e softwares decorrentes;
- 8.3.1.2.2. ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos do CONTRATANTE;
- 8.3.1.2.3. o processo de construção, no ambiente do CONTRATANTE e demais órgãos, dos mecanismos de criptografia e autenticação utilizados;
- 8.3.1.2.4. informações de banco de dados do Tribunal que a CONTRATADA possa ter acesso;
- 8.3.1.2.5. caso haja processamento de dados pessoais neste TR e no contrato, realizá-la em cumprimento às determinações da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

### 8.4. DA FISCALIZAÇÃO

8.4.1. A atuação ou a eventual omissão da fiscalização durante a realização dos trabalhos, não poderá ser invocada para eximir a CONTRATADA da responsabilidade no fornecimento dos serviços;

8.4.2. Caso identificados serviços em execução que não estejam, comprovadamente, sendo executados de maneira satisfatória, conforme especificações da contratação, o TRE-DF poderá rejeitar ou sustar a execução de serviços insatisfatórios, exigindo que estes sejam refeitos;

8.4.3. A gestão do contrato será exercida por servidor da Secretaria de Tecnologia da Informação (STIC), nas questões técnicas referentes a tecnologia da informação, e da Assessoria de Fiscalização de Contratos (AFIC), nas questões jurídicas/administrativas, através das informações fornecidas pela CONTRATADA e pelo fiscal/gestor do contrato;

8.4.4. A ação ou omissão, total ou parcial, de fiscalização ou gestão do TRE-DF não restringe e nem exige a CONTRATADA a total responsabilidade pelos encargos e serviços que são de sua atribuição e competência, nem mesmo das obrigações assumidas neste instrumento.

### 8.5. DOS CRITÉRIOS DE ACEITAÇÃO E RECEBIMENTO

8.5.1. As credenciais e as liberações de acesso aos Serviços de Suporte Técnico de Software Oracle deverão estar disponíveis em no máximo 10 (dez) dias corridos a contar do 1º dia útil seguinte a data inicial da vigência contratual;

8.5.2. O **recebimento do objeto** será realizado da seguinte forma:

- 8.5.2.1. **Provisoriamente**, assim que efetuada a ativação das credenciais e liberação de acesso aos Serviços de Suporte Técnico de Software Oracle, para efeito de posterior verificação da conformidade com as especificações;
- 8.5.2.2. **Definitivamente**, até 10 (dez) dias úteis da efetiva ativação das credenciais e liberação de acesso aos Serviços de Suporte Técnico de Software Oracle, após verificação da qualidade e quantidade do serviço/produto e consequente aceitação.

8.5.3. **Consideradas insatisfatórias** as condições do objeto recebido provisoriamente, em relação ao acesso do ambiente de suporte técnico, será lavrado Termo de Recusa, no qual serão consignadas as desconformidades, devendo a ativação das credenciais e liberação de acesso aos Serviços de Suporte Técnico de Software Oracle serem regularizadas no prazo máximo de 03 (três) dias úteis a partir da comunicação oficial feita pelo TRE-DF, sem qualquer custo adicional para o CONTRATANTE;

8.5.4. Após a **notificação** à CONTRATADA, o prazo decorrido até então será desconsiderado, iniciando-se nova contagem para o recebimento definitivo, tão logo sanada a situação;

8.5.5. O recebimento provisório e definitivo do objeto **não exclui a responsabilidade civil a ele relativa, nem a ético-profissional**, dar-se-á a inexecução e possível cancelamento se não satisfeitas às seguintes condições:

- 8.5.5.1. Objeto em acordo com a especificação técnica contidas no Termo de Referência e na Proposta Comercial;
- 8.5.5.2. Quantidades em conformidade com o estabelecido no Termo de Contrato;

8.5.6. Entrega no prazo, e a conformidade entre o período da vigência e o estabelecido no ambiente do Suporte Técnico do fabricante previstos no Termo de Referência.

### 8.6. DAS SANÇÕES

8.6.1. As sanções estão previstas na minuta do Termo de Contrato.

### 8.7. DO PAGAMENTO

8.7.1. A CONTRATADA deverá apresentar **Nota Fiscal/Fatura** para liquidação e pagamento da despesa pelo TRE-DF, após realizado o aceite definitivo pela equipe técnica.

8.7.2. O pagamento deve atender ao estipulado no IMR, no item 7.3 deste TR.

8.7.3. Demais condições estão previstas na minuta do Termo de Contrato.

### 8.8. DO LOCAL

8.8.1. Os serviços prestados pela CONTRATADA serão executados nos computadores/servidores da Sede do TRE-DF, localizada na Praça Municipal - Qd. 02, Lote 06, Brasília - DF - Brasil.

## 9. DOTAÇÃO ORÇAMENTÁRIA

9.1. A despesa classifica-se na Ação 21EE: PO SEG0 - Segurança da Informação, na natureza de despesa 3390.40 - 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).

#### 10. ESTIMATIVA E VALOR DA CONTRATAÇÃO

10.1. Conforme o item 2.7.5.3 deste Termo de Referência, o **valor estimado total na vigência do contrato** é de R\$ 724.578,24 (setecentos e vinte e quatro mil quinhentos e setenta e oito reais e vinte e quatro centavos), com **pagamentos mensais estimados em R\$ 12.076,30 (doze mil setenta e seis reais e trinta centavos)**.

#### 11. GARANTIA CONTRATUAL:

11.1. A contratada prestará garantia de execução do contrato, nos moldes do art. 96 e seguintes, da Lei nº 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor anual do contrato, conforme o par. único do art. 98 da mesma Lei.

11.2. Em caso de renovação da contratação, após os 60 meses, será necessário prestar nova garantia contratual, cuja cobertura abrangerá o novo período renovado.

#### 12. VIGÊNCIA DO CONTRATO E PRORROGAÇÃO:

12.1. A vigência contratual será de 60 meses, prorrogáveis por igual período, conforme o art. 107 da Lei nº 14.133/2021.

#### 13. DO REAJUSTE:

13.1. O índice de reajuste será estipulado de acordo com a variação do menor índice de inflação, salvo variação negativa, tendo por base o ICTI/IPEA, admitindo-se, ainda, a livre negociação entre os contratantes, sempre no sentido de se obter preço mais vantajoso para a Administração, em atenção aos princípios da eficiência e da economicidade, observada a periodicidade estabelecida no artigo 92, §4º, inc. I, da Lei nº 14.133/2021.

#### 14. MODELOS (TEMPLATES)

##### 14.1. ORDEM DE FORNECIMENTO - ANEXO I

##### 14.2. TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO / DECLARAÇÃO DE CIÊNCIA - ANEXO II

##### 14.3. TERMO DE CIÊNCIA DA POLÍTICA DE GERENCIAMENTO DE CRISES CIBERNÉTICAS E DA POLÍTICA DE ACESSO AOS RECURSOS DE TIC (PARTIC) - ANEXO III

A Equipe de Planejamento da Contratação, composta pelos **Integrantes Demandante, Técnico e Administrativo**, designados por meio da Decisão 166 (id 1037108), abaixo elencados, **assina e data este documento eletronicamente e por meio de despacho posterior confirmatório** :

Equipe de Planejamento da Contratação	
_____ Diego Batista Assunção do Vale Matrícula: 1971 Integrante Demandante	_____ Leandro Amorim Carisio Matrícula: 2131 Integrante Técnico
_____ Rafael Dittberner Matrícula: 0562 Integrante Administrativo	

### ANEXO I

#### ORDEM DE FORNECIMENTO

**ORDEM DE FORNECIMENTO N°** \_\_\_\_

**PA SEI id.** \_\_\_\_\_

**Objeto:** Contratação de empresa para a prestação de serviços de suporte técnico e atualização de licenças do Banco de dados Oracle

**Contratante:** Tribunal regional Eleitoral do Distrito Federal - TREDF

**Contratada:** ORACLE DO BRASIL

Por este instrumento, autorizo o início do fornecimento, em conformidade com o especificado no Termo de Referência e correspondente instrumento contratual, devendo ser concluído no prazo máximo de \_\_\_\_ dias corridos, contados do envio da Ordem de Fornecimento.

Local da entrega: sede do Tribunal Regional Eleitoral do Distrito Federal, situado na Praça Municipal Quadra 02, Lote 06, Brasília-DF, Térreo, edifício Anexo, no horário das 13h às 18h.

Telefone: (61) 3048-\_\_\_\_\_.

Brasília-DF, \_\_\_\_\_ de \_\_\_\_\_ de 2023.

**CONTRATANTE:**

Gestor do Contrato: \_\_\_\_\_

Matrícula: \_\_\_\_\_

**CONTRATADA:**

Recebido e de acordo, Brasília-DF, \_\_\_\_\_ de \_\_\_\_\_ de 2023.

Preposto: \_\_\_\_\_

**ANEXO II****TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO**

O TRIBUNAL REGIONAL ELEITORAL DO DISTRITO FEDERAL, sediado na Praça Municipal - Qd. 02, Lote 06, Brasília - DF - Brasil, CEP: 70.094-901, CNPJ n.º 04.099.695/0001-61 doravante denominado CONTRATANTE, e, de outro lado, a Oracle do Brasil Sistemas Ltda., sediada em Rua Dr. José Aureo Bustamente, n.º 455, Morumbi Business Center, Vila São Francisco, CEP 04.710-090, CNPJ n.º 59.456.277/0001-76, doravante denominada CONTRATADA; CONSIDERANDO que, em razão do CONTRATO N.º XX/2024 doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

**CLÁUSULA PRIMEIRA – DO OBJETO**

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto n. 7.845/2012 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

**CLÁUSULA SEGUNDA – DOS CONCEITOS E DEFINIÇÕES**

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

**Informação:** é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

**Informação Pública ou Ostensiva:** são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

**Informações Sensíveis:** são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

**DECLARAÇÃO DE CIÊNCIA DO TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**

Por meio desta, o(a) Sr(a) [nome do(a) diretor, consultor, prestador de serviço, empregado ou preposto], CPF \_\_\_\_\_, ocupante do cargo [cargo que ocupa] na empresa [Nome (Razão Social) da empresa], CNPJ [número do CNPJ da empresa], declara sob as penas da Lei, ter tomado conhecimento do TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS), emitido por ocasião da assinatura do contrato n.º \_\_\_\_\_/2024, e se compromete a seguir, naquilo que lhe couber, todas as disposições do referido Termo.

Local e data,

\_\_\_\_\_  
Assinatura

**ANEXO III**

**TERMO DE CIÊNCIA DA POLÍTICA DE GERENCIAMENTO DE CRISES CIBERNÉTICAS E DA POLÍTICA DE ACESSO AOS RECURSOS DE TIC (PARTIC)**

Por meio desta, o(a) Sr(a) [nome do(a) diretor, consultor, prestador de serviço, empregado ou preposto], CPF \_\_\_\_\_, ocupante do cargo [cargo que ocupa] na empresa [Nome (Razão Social) da empresa], CNPJ [número do CNPJ da empresa], declara sob as penas da Lei, ter tomado conhecimento da POLÍTICA DE GERENCIAMENTO DE CRISES CIBERNÉTICAS, disposta na Portaria Presidência nº 1/2022, bem como da POLÍTICA DE ACESSO AOS RECURSOS DE TIC (PARTIC), disposta na Portaria Presidência nº 27/2022, e se compromete a observá-las, naquilo que lhe couber.

Local e data,

\_\_\_\_\_  
Assinatura



Documento assinado eletronicamente por **LEANDRO AMORIM CARISIO, Chefe de Seção**, em 09/04/2024, às 12:27, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **RAFAEL DITBERNER, 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](https://sei.tre-df.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código verificador **1590107** e o código CRC **397DCAE3**.