TRIBUNAL REGIONAL ELEITORAL DO CEARÁ

ESTUDOS PRELIMINARES DE CONTRATAÇÃO DE TIC

PROCESSO SEI TRE/CE Nº 2022.0.000000625-5

Histórico do documento

Data	Versão	Descrição	Autor(es)
18/05/2022	1.0a	Minuta elaborada pela equipe do TRE/ES	Juliana Kowata (TRE/ES)
20/06/2022	1.5a	Versão adaptada pela equipe do TRE/CE	Jonas Luz Jr. (TRE/CE)
08/07/2022	2.0a	Minuta atualizada pela equipe do TRE/ES	Juliana Kowata (TRE/ES)
28/07/2022	2.5	Versão atualizada pela equipe do TRE/CE	Jonas Luz Jr. (TRE/CE)
10/08/2022	3.0	Versão ajustada após ressalvas da Assessoria Jurídica - ASDIR (SEI nº 0015297)	Jonas Luz Jr. (TRE/CE)
15/08/2022	3.1	Versão ajustada, com a identificação correta dos integrantes da EPC	Jonas Luz Jr. (TRE/CE)
17/08/2022	3.5	Versão corrigida, com ajustes indicados pela equipe técnica do TRE/ES.	Jonas Luz Jr. (TRE/CE)
24/08/2022	3.6	Versão com correção de erros de digitação, identificados pelo representante técnico do TRE/CE	Jonas Luz Jr. (TRE/CE)
13/09/2022	4.0	Versão com ajustes determinados pela ASGES e retificações de quantitativos enviadas pelos Tribunais Participantes.	Jonas Luz Jr. (TRE/CE)

1. Introdução

Este documento apresenta o estudo técnico preliminar, que constitui primeira etapa do planejamento de uma contratação (planejamento preliminar) e serve essencialmente para assegurar a viabilidade técnica da contratação e embasar o termo de referência ou o projeto básico, conforme previsto na Lei 8.666/1993, art. 6°, inciso IX. Além disso, é requisito da Resolução CNJ Nº 182/2013[1] que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ). A estrutura deste documento baseia-se nas orientações constantes do Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação[2] , publicado pelo Tribunal de Contas da União.

1.1. Equipe de Planejamento da Contratação

Equipe	
Integrantes Demandantes:	**TRE/ES:** JANINE VENTURINI DE REZENDE (substituto: JULIANA HIROKO KOWATA) **TRE/CE:** JONAS DE ARAÚJO LUZ JUNIOR
Integrantes Técnicos:	**TRE/ES:** JULIANA HIROKO KOWATA (substituto: JANINE VENTURINI DE REZENDE) **TRE/CE:** THIAGO PAGELS COSTA
Integrantes Administrativos:	**TRE/CE:** JONAS DE ARAÚJO LUZ JUNIOR

2. Caracterização da demanda

2.1. Descrição sucinta

Aquisição de licenças de software de segurança da informação, com direitos de suporte e de atualização destes programas, para os bancos de dados do Oracle Database hospedados nos tribunais participantes.

2.2. Qualificação e alinhamento estratégico da demanda

A qualificação da demanda e seu alinhamento estratégico estão documentados no DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA (DOD) Nacional v. 1.1 (SEI nº 0017383)

2.3. Fundamentação legal

1. **Lei nº 13.709/2018**[3] : Lei Ge**ral de Proteção de Dados (LGPD);**
2. **Decreto nº 9.637/2018**[4] : Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
3. **Resolução CNJ nº 363/2021**[5] : Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;
4. **Resolução TSE nº 23.650/2021**[6] : Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;
5. **Resolução TSE nº 23.644/2021**[8] : Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

6. **Instrução Normativa SGD-ME nº 1/2019**[9] : Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

2.4. Referências Técnicas

1. **NBR ISO/IEC 27001:2013;**
2. **NBR ISO/IEC 27002:2013;**
3. **NBR ISO/IEC 27005:2019.**

2.5. Justificativa da Necessidade

Necessidade 01: Aprimorar medidas técnicas de segurança da informação visando defesa, proteção e monitoramento de dados organizacionais nos bancos de dados Oracle hospedados nos sítios dos Tribunais contratantes e assegurar que estejam em conformidade com os normativos relacionados na seção Fundamentação legal.

Necessidade 02: Assegurar às equipes de administradores de banco de dados Oracle o instrumental adequado para a condução de projetos em convergência com a Estratégia Nacional de Cibersegurança de TIC da Justiça Eleitoral, bem como operacionalizar diretrizes e recomendações da Política de Segurança a Informação.

2.6. Resultados Esperados

R01: Prevenção, detecção e auditoria de incidentes de segurança da informação nos bancos de dados Oracle:

a. Prevenção ativa contra acessos indevidos;
b. Prevenção ativa contra execução de comandos maliciosos a partir de acessos autorizados;
c. Restrição prévia de acessos indevidos, baseada em política de segurança que envolva restrições de acesso de horário, endereços IP, aplicações, contas;
d. Detecção, em tempo real, de tentativas de violação de política de segurança;
e. Coleta unificada de auditoria de dados sensíveis, com histórico de acessos.

R02: Redução de probabilidade de exposição de dados dos bancos de dados Oracle:

a. Proteção contra exposição de dados decorrentes de roubo, perda, sequestro de mídia de armazenamento e backups de banco de dados roubados ou perdidos;
b. Proteção na entrega de dados a terceiros, garantindo o acesso somente a quem de direito;
c. Restrição de visualização de dados sensíveis diretamente na requisição de dados, sem que haja necessidade

de revisão de sistemas corporativos que o acessam, ou seja, sem alteração do código-fonte;

d. Restrição de visualização de dados sensíveis por ferramentas de acesso direto ao banco de dados;
e. Redução de pontos com replicação de dados originados no ambiente produtivo;

R03: Redução de danos ou ações maliciosas originadas de dentro do órgão:

a. Proteção contra abusos e ataques gerados a partir de "contas de administração";
b. Proteção contra erros ocasionados por excesso de privilégios;
c. Proteção contra ataques e roubos originados por acessos autorizados;
d. Redução de danos em caso de extravio ou divulgação de contas de administração.

3. Especificação dos Requisitos

3.1. Requisitos de Negócio

Id	Requisito
RN.001	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.

3.2. Requisitos legais

Id	Requisito	Fundamento Legal
RL.001	A solução deverá estar alinhada com os normativos elencados na seção "Fundamentação Legal" e as boas práticas das "Referências Técnicas" consideradas para a presente contratação.	Vide "Fundamentação Legal" e "Referências Técnicas"
RL.002	A solução deverá proteger dados de acessos não autorizados.	LGPD, Art. 6º, VII LGPD, Art. 46 CNJ nº 363/2021XI TSE nº 23650/2021, Art. 8º, V Resolução nº 23.644/2021, Art. 7º II-b, Art. 20-III
RL.003	A solução deverá proteger dados de situações acidentais de destruição, perda, alteração, comunicação ou difusão.	LGPD, Art. 6º, VI LGPD, Art. 46I
RL.004	A solução deverá prevenir ocorrência de danos em virtude do tratamento de dados.	LGPD, Art. 6º, VIII
RL.005	A solução deverá ser capaz de comprovar a observância e o cumprimento de normas de proteção de dados.	LGPD, Art. 6º, X TSE nº 23650/2021, Art. 7º, Parágrafo Único
RL.006	A solução deverá ser capaz de tornar os dados pessoais anônimos de modo não reversível.	LGPD, Art. 12, § 3º LGPD, Art. 16, II e IV
RL.007	A solução deverá ser capaz de manter registro de auditoria das operações de tratamento de dados.	LGPD, Art. 37, II e IV TSE nº 23650/2021, Art. 8º, VI
RL.008	A solução deverá informar sobre tentativa de violação de política de segurança.	LGPD, Art. 48, § 1º TSE nº 23650/2021, Art. 8º, VIII TSE nº 23650/2021, Art. 15º, III; Art. 17º, IV Resolução nº 23.644/2021, Art. 7º, V Resolução nº 23.644/2021, Art; 14, § 2º
RL.009	A solução deverá manter registro de auditoria de tentativa de violação ou violação de política de segurança.	LGPD, Art. 48, III
RL.010	A solução deverá permitir adoção de medidas técnicas para tornar os dados ininteligíveis para terceiros não autorizados a acessá-los.	LGPD, Art. 48, § 3º TSE nº 23650/2021, Art. 14, IV
RL.011	A solução deverá permitir medidas tais como a aposição de tarjas sobre dados pessoais ou a supressão parcial de números cadastrais.	TSE nº 23650/2021, Art. 7º, Parágrafo Único

Id	Requisito	Fundamento Legal
RL.012	A solução deverá permitir o uso de recursos criptográficos sobre os bancos de dados	Resolução nº 23.644/2021, Art. 9º, IIk, Art. 17.
RL.013	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 9.279/1996 Lei 9.609/1998

2.3. Requisitos Funcionais

2.3.1. Criptografia de Dados

Referência Legal: RL.001, RL.002, RL.003, RL.010, RL.012

Id	Requisito
RF.CRP.001	A solução deverá 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*.
RF.CRP.002	A solução deverá apresentar os dados descriptografados, de forma transparente quando acessados 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.
RF.CRP.003	A solução deverá 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.
RF.CRP.004	A solução deverá 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.
RF.CRP.005	A solução deverá permitir a escolha do tamanho da chave criptográfica e o algoritmo nas operações de criptografia, oferecendo, minimamente: 3DES168, AES128, AES192,AES256.
RF.CRP.006	A solução deverá ser capaz de utilizar chaves criptográficas armazenadas no Oracle wallet, nos padrões PKCS#12 e PKCS#5.
RF.CRP.007	A solução deverá 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.
RF.CRP.008	A solução deverá permitir a escolha da granularidade da operação de criptografia, possibilitando, minimamente, a seleção de coluna ou *tablespaces* que serão criptografados.
RF.CRP.009	A solução deverá 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.
RF.CRP.010	A solução deverá ser completamente integrada ao Oracle *Database*, com suporte à aceleração de criptografia baseada em hardware, compatível com tecnologia Intel® Advanced Encryption Standard Instructions (AES-NI)
RF.CRP.011	A solução deverá 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.
RF.CRP.012	A solução deverá se capaz de utilizar de chaves de criptografia de padrões PKCS#12 e PKCS#5
RF.CRP.013	A solução deverá permitir a compressão de dados em dados criptografados.
RF.CRP.014	A solução não deverá impedir o uso de transportable tablespace para dados criptografados.
RF.CRP.015	A solução não deve ter limitações quanto ao tipo e quanto ao tamanho do dado a ser criptografado.
RF.CRP.016	A solução não deve solicitar o aumento de espaço de armazenamento utilizado, em função de eventual overhead no processo de criptografia.

2.3.2. Reescrita de Dados

Referência Legal: RL.001, RL.002, RL.003, RL.010, RL.012

Id	Requisito
RF.RED.001	A solução deverá 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.
RF.RED.002	A solução deverá 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.

Id	Requisito
RF.RED.003	A solução deverá ser capaz de realizar a reescrita do dado, minimamente, nos seguintes modos: **Completo:** Reescreverá todo o dado. Ex.: Se o CPF for 455.821.052-39, a solução não deve exibir nenhum dígito real. **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. **Por expressões regulares:** Reescreverá o dado mediante casamento de padrões de texto. Ex.: reescrever parte de email baseado na expressão regular do domínio. De joao@tre-es.gov.br para ***@****.gov.br **Aleatório:** Reescreverá o dado de forma aleatória a cada consulta. **Nenhum:** Não haverá reescrita alguma sobre o dado.
RF.RED.004	A solução deverá reescrever o dado entregue para a consulta, sem afetar o dado armazenado no Oracle Database.
RF.RED.005	A solução deverá reescrever o dado consultado em tempo de execução.
RF.RED.006	A solução deverá prover critérios de reescrita flexíveis, considerando o contexto da sessão do usuário de banco responsável pela consulta.
RF.RED.007	A solução deverá permitir a criação de várias políticas de reescrita de dados
RF.RED.008	A solução deverá ser capaz de reescrever dados dos seguintes tipos, minimamente: Caracters: CHAR, VARCHAR2 (incluindo VARCHAR2 longos, por exemplo, VARCHAR2(20000)), NCHAR, NVARCHAR2, Dígitos: NUMBER, FLOAT, BINARY_FLOAT, BINARY_DOUBLE Brutos: LONG RAW, RAW Data: DATE, TIMESTAMP, TIMESTAMP WITH TIME ZONE, TIMESTAMP WITH LOCAL TIME ZONE Intervalos: INTERVAL YEAR TO MONTH, INTERVAL DAY TO SECOND

2.3.3. Mascaramento de Dados e Seleção de Subconjunto de Dados

Referência Legal: RL.001;RL.002; RL.003;RL.005;RL.006;RL.010

Id	Requisito
RF.MSK.001	A solução deverá 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.
RF.MSK.002	A solução deverá prover, minimamente, as seguintes transformações sobre os dados: **Mascaramento Condicional:** consiste em utilizar diferentes formatos de mascaramento a partir de condições preestabelecidas. **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. **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. **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. **Mascaramento reversível baseado em chave:** consiste em criptografar e descriptografar os dados originis, utilizando uma chave segura. 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.
RF.MSK.003	A solução deve permitir a segregação de privilégios de administração, mascaramento de dados e de criação de amostras de dados.
RF.MSK.004	A solução deve permitir o mascaramento e a produção de amostras quando em uso da ferramenta Oracle Database – *Data Pump*.
RF.MSK.005	A solução deve 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
RF.MSK.006	A solução deverá 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.
RF.MSK.007	A solução deverá permitir a visualização do resultado do mascaramento e da amostra antes de efetivamente criá-los.
RF.MSK.008	A solução deverá 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.
RF.MSK.009	A solução deverá ser integrada ao Oracle Database, sem a necessidade de uso de ferramentas de terceiros.
RF.MSK.010	A solução deverá permitir que os critérios utilizados na geração de uma determinada amostra possa ser gravada, de modo que a operação possa ser repetida inúmeras vezes.

Id	Requisito
RF.MSK.011	A solução deverá prover mecanismos que auxiliem na identificação de dados sensíveis.

2.3.4. Controle de Acesso

Referência Legal: RL.001;RL.002; RL.003;RL.004

Id	Requisito
RF.CAC.001	A solução deverá ser 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.
RF.CAC.002	A solução deverá ser 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.
RF.CAC.003	A solução deverá ser capaz de separar os papéis do administrador de políticas de segurança do papel de administrador de contas de usuários.
RF.CAC.004	A solução deverá ser 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.
RF.CAC.005	A solução deverá ser 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*)
RF.CAC.006	A solução deverá ser 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.
RF.CAC.007	A solução deverá ser capaz de habilitar ou desabilitar *roles* para contas de usuário baseado na avaliação resultante do conjunto de regras.
RF.CAC.008	A solução deverá possuir uma biblioteca de funções e procedimentos que permitam ao administrador da solução flexibilidade na definição de regras de segurança.
RF.CAC.009	A solução deverá armazenar as informações de configuração, tais como zonas segura, conjunto de regras, regras, de forma a possibilitar consulta posterior.
RF.CAC.010	A solução deverá garantir compatibilidade com as demais funcionalidades de segurança que tratam de criptografia, mascaramento de dados e reescrita de dados.

2.3.5. Auditoria de Atividades e Monitoramento de Instruções no Banco de Dados

Referência Legal: RL.001;RL.002; RL.003;RL.004, RL.007, RL.008, RL.009

Id	Requisito
RF.AEM.001	A solução deverá ser capaz de capturar informações detalhadas de usuários e aplicações de banco de dados, incluindo usuários com privilégios administrativos elevados.
RF.AEM.002	A solução deverá ser capaz de capturar informações sobre mudanças críticas nos bancos de dados, modificações em contas, mudanças de autorização, eventos de login e logout.
RF.AEM.003	A solução deverá ser capaz de emitir alertas sobre eventos específicos como tentativa excessiva de logins, acesso a dados sensíveis por usuários não autorizados e operações de exportação de dados.
RF.AEM.004	A solução deverá ser capaz de capturar valores antes e depois de mudanças.
RF.AEM.005	A solução deverá permitir a importação de arquivo contendo a identificação de dados sensíveis de modo que permita a associação de regras de auditoria específicas para esses elementos.
RF.AEM.006	A solução deverá ser capaz de monitorar ativamente o tráfego de instruções SQL que chegam ao banco de dados e determinar com precisão se permitirá, registrará, alertará, substituirá ou bloqueiará a instrução.
RF.AEM.007	A solução deverá ser capaz de analisar o tráfego de instruções SQL incluindo verificações de endereços IP, usuário de banco de dados e de sistema operacional, nome de programa, categoria da instrução (DML/DDL) e tabelas acessadas.
RF.AEM.008	A solução deverá ser capaz de bloquear e ou alertar sobre instruções que estão na lista de negação e instruções que não estão na lista permitida, auxiliando a prevenir ataques de injeção SQL.
RF.AEM.009	A solução deverá prover recursos para monitorar e alertar sobre tentativas de exfiltração de dados (transferência não autorizada de dados).
RF.AEM.010	A solução deverá ser capaz de identificar equivalência entre instruções SQL definidas na política de segurança.
RF.AEM.011	A solução deverá ser capaz de auditar e monitorar diversos bancos de dados simultaneamente.
RF.AEM.012	A solução deverá apresentar um painel de controle de atividades para facilitar a interação entre os administradores da solução e os alertas de auditoria e monitoramento.
RF.AEM.013	A solução deverá ser capaz de monitorar tráfego de dados originado de/destinado a um Oracle Database quando a criptografia Oracle Native Network for utilizada.
RF.AEM.014	A solução deverá ser capaz de substituir uma instrução SQL por outra.

2.4. Requisitos de Capacitação

Id	Requisito
RC.001	A solução deverá estar acompanhada de documentação elaborada na forma de guias de utilização, contendo informações de nível básico ao avançado.
RC.002	A solução deverá contar com suporte técnico 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.

2.5. Requisitos Ambientais

Id	Requisito
RA.001	A solução deverá se conformar ao ambiente tecnológico e físico que está em operação na contratante.
RA.002	A solução, as atualizações evolutivas e/ou corretivas devem ser distribuídas de forma digital e on-line, sempre que disponíveis.

2.6. Requisitos Culturais

Id	Requisito
RC.001	A solução não deverá impedir o uso das ferramentas já utilizadas para a administração de banco de dados.
RC.002	A solução deverá priorizar o idioma Português Brasil sempre que possível e na sua ausência, o idioma Inglês (EUA).

2.7. Requisitos Sociais

Id	Requisito
RS.001	A solução não deverá impedir o exercício das funções do contratante ou gerar a indisponibilidade dos serviços por ele prestados.

2.8. Requisitos de Manutenção e Garantia

Id	Requisito
RM.001	A solução deve fornecer atualizações que corrijam falhas de segurança pelo período contratado, que deve ser de, pelo menos, 12 meses, renovável até o limite permitido em lei.
RM.002	A solução deve fornecer canal digital, disponível a qualquer hora do dia, de domingo a sábado, para contato com suporte técnico.
RM.003	A solução deverá garantir compatibilidade com versões de banco de dados que estejam dentro do ciclo de vida de suporte do Oracle Database.
RM.004	A solução deverá apresentar possibilidade de atualização de versão sem perda de histórico ou de configuração existente.
RM.005	A solução deverá permitir o acesso simultâneo de vários técnicos do contratante ao suporte técnico, atendendo às demandas individualmente.

2.9. Requisitos Temporais

Id	Requisito
RT.001	A fabricante da solução deverá prestar suporte técnico e disponibilizar versões de atualização e correção pelo período contratado, que deve ser de, pelo menos, 12 meses.

2.10. Requisitos de Segurança da Informação

Id	Requisito
RS.001	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.
RS.002	A contratada deverá fornecer credenciais seguras para a contratante a fim de acessar o suporte técnico e as atualizações de versão.
RS.003	A contratante poderá alterar a senha de acesso ao suporte técnico e às atualizações sempre que considerar conveniente, sem necessidade de anuência da contratada.
RS.004	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.
RS.005	A contratada deverá se comprometer a manter sigilo das informações do Tribunal Contratante a que tiver acesso, devendo, a contratada, assinar Termo de Compromisso e Manutenção de Sigilo, bem como manifestar, por escrito, ciência do Código de Ética, o qual deverá seguir.

2.11. Requisitos de Arquitetura Tecnológica

Id	Requisito
RC.ARQ.001	A solução deverá ser compatível com as configurações e ambiente da contratante descritos no *Anexo D*.
RC.ARQ.002	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.
RC.ARQ.003	A solução deverá ser compatível com arquitetura multi-tenant e também para arquitetura non-cdb do Oracle Database.

3. Descrição da Solução de TIC

3.1. Elementos da STIC

A solução de TI é composta pelos seguintes elementos, que de forma integrada, contribuirá para o alcance dos resultados esperados da contratação:

a. Licenças de um ou mais produtos de software para segurança da informação de banco de dados Oracle hospedados nos tribunais participantes;

b. Documentação: guias de administração e uso do(s) produto(s) de software(s);

c. Serviço de suporte técnico por 12 (doze) meses;

d. Serviço de atualização de versão do(s) produto(s) de software por 12 (doze) meses.

4. Avaliação das Soluções de Tecnologia da Informação

4.1. Análise de Aderência ao Requisitos Funcionais

Os requisitos funcionais da solução de tecnologia da informação a ser contratada foram agrupados conforme os seguintes mecanismos de segurança:

a. Criptografia de dados (CRP);

b. Reescrita de dados (RES);

c. Mascaramento de dados e seleção de subconjunto de dados (MSK);

d. Controle de acesso (CAC);

e. Auditoria de atividades e monitoramento de instruções no banco de dados (AEM).

Os produtos de software a seguir foram identificados e classificados em relação aos requisitos funcionais:

Quadro 1. Análise de produtos de software

Seq.	Produto de Software	Fabricante	Uso	Referência	CRP	RES	MSK	CAC	AEM
1	DB Protect	Trustwave	Licença	https://support.trustwave.com/software/Database-Security/DbProtectInstallGuide_6.4.9.pdf	N	N	N	P	P
2	Fogger	TheSoftwareHouse	OpenSource	https://github.com/TheSoftwareHouse/fogger	N	N	P	N	N
3	Heimdall Data	Heimdall Data	Subscription	https://www.heimdalldata.com/	N	N	N	N	P
4	IBM Security™ Guardium Data Guard Encryption	IBM	Licença	https://www.ibm.com/downloads/cas/DV7O2GZN	P	N	N	P	S
5	IBM Security™ Guardium Data Protection	IBM	Licença	https://www.ibm.com/products/ibm-guardium-data-protection	N	N	N	S	P
6	Imperva SecureSphere	IBM	Licença	https://www.ibm.com/docs/en/dsm?topic=configuration-imperva-securesphere	N	N	N	P	S
7	Oracle Advanced Security	Oracle	Licença	https://docs.oracle.com/en/database/oracle/oracle-database/21/asoag/security-considerations-for-using-oracle-data-redaction.html	S	S	N	N	N
8	Oracle Audit Vault & Database Firewall	Oracle	Licença	https://docs.oracle.com/en/database/oracle/audit-vault-database-firewall/20/sigig/preface.html https://www.oracle.com/br/database/technologies/security/audit-vault-firewall.html	N	N	N	S	S
9	Oracle Data Masking and Subsetting Pack	Oracle	Licença	https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dmksb/index.html	N	N	S	N	N
10	Oracle Database Vault	Oracle	Licença	https://docs.oracle.com/en/database/oracle/oracle-database/21/dvadm/introduction-to-oracle-database-vault.html	N	N	N	S	N
11	ProxySQL	ProxySQL	Licença	https://proxysql.com/	N	N	N	N	N
12	Sonar	Imperva	Licença	https://www.imperva.com/products/database-risk-compliance	N	N	N	P	P

Legenda: Atendimento aos requisitos funcionais: S – Atende / N – Não atende/ P – Atende Parcialmente

4.2. Análise das Soluções de Mercado

O *Quadro 1. Análise de produtos de software* apresenta uma relação de produtos de software voltados para a segurança da informação, identificados no mercado, para cada grupo de requisitos. À direita, segue análise qualitativa de conformidade de produtos de software identificados no mercado aos requisitos funcionais especificados para esta contratação.

A análise dos dados apresentados permite constatar que os produtos de software tem atuação altamente especializada, abarcando um ou dois grupos de requisitos funcionais. Portanto, a solução de TIC, com vistas a alcançar os resultados esperados da contratação, será composta por diferentes produtos de software que deverão ser orquestrados dentro da infraestrutura da contratante.

Para a escolha dos produtos de software, os critérios a seguir foram considerados:

a. A configuração do conjunto de módulos e produtos que compõem a STIC necessita atender os requisitos de arquitetura, com destaque para os requisitos: o RT.ARQ.002 que trata da compatibilidade entre os componentes da solução e o RT.ARQ.003 que trata de arquitetura específica do Oracle Database Enterprise Edition;

b. As candidatas preferenciais serão aquelas que atenderem completamente os requisitos especificados;

c. A contratação de produtos de mesmo fabricante será privilegiada, quando se mostrar viável e não reduzir a concorrência, pois há uma complexidade inerente em se compatibilizar o uso de produtos de diferentes fabricantes, assim como é conhecido que na interlocução com diferentes fabricantes ocorrem conflitos de competência e de delimitação de responsabilidades.

Dos produtos elencados, os requisitos funcionais agrupados nos mecanismos de segurança “Criptografia de dados” (CRP), “Reescrita de dados” (RES), “Mascaramento de dados e seleção de subconjunto de dados” (MSK) e

"Controle de acesso" (CAC) são contemplados nos programas distribuídos em conjunto com o produto de software *Oracle Database Enterprise Edition* e, portanto, já se encontram instalados na infraestrutura tecnológica dos tribunais: *Oracle Advanced Security*, *Oracle Data Masking and Subsetting Pack* e *Oracle Database Vault*. Estes programas são denominados de *"options"* ou *"packs"* porque são opcionais de segurança nativos do próprio ecossistema Oracle, estendendo as funcionalidades de segurança do banco Oracle, ao qual já estão incorporados, requerendo, todavia, aquisição de licenças específicas de uso.

Para os critérios apontados, a adoção dos referidos produtos de segurança nativos para o *Oracle Database EE*, favorece:

a. Garantia de suporte e compatibilidade entre as versões dos produtos de segurança e a do próprio SGBD, por integrarem a sua arquitetura e acompanharem seu calendário do ciclo de vida;

b. Minimização de sobrecarga decorrente de integração entre diferentes produtos, pois se integram aos recursos de forma nativa, atuando como verdadeiras extensões de funcionalidade do *Oracle Database Enterprise Edition*;

c. Redução do impacto cultural, uma vez os produtos observam os paradigmas e conceitos da arquitetura Oracle com a qual as equipes técnicas (desenvolvedores, DBAs, etc.) estão ambientadas;

d. Redução de necessidade de intervenção no ambiente tecnológico, considerando que alguns dos produtos já se encontram instalados e acessíveis para uso; e

e. Reconhecimento automático das extensões de segurança pelas interfaces de administração do *Oracle Database* que são utilizadas pelos administradores do SGBD.

Portanto, adotando, fundamentalmente, os critérios de aderência à padronização do ambiente de desenvolvimento e operação dos bancos de dados na Justiça Eleitoral e risco praticamente nulo de incompatibilidade dos produtos com o SGBD alvo da contratação, associados, secundariamente, aos critérios de simplicidade de instalação e manutenção, os produtos *Oracle Advanced Security*, *Oracle Data Masking and Subsetting Pack* e *Oracle Database Vault* apresentam-se como os recomendados para atender aos requisitos funcionais dos grupos CRP, RES, MSK e CAC.

Os requisitos funcionais agrupados no mecanismo de segurança da Informação "Auditoria de atividades e monitoramento de instruções no banco de dados" (AEM) são atendidos pelo *Oracle Audit Vault & Database Firewall*, produto específico distribuído separadamente do *Oracle Database Enterprise Edition* na forma de *"soft appliance"*, ou seja, um conjunto empacotado ou pré-configurado com definições de hardware (servidores, memória, armazenamento, canais de I/O), software (sistema operacional e software de gerenciamento) e conectividade (interfaces de rede) que deve ser incorporado à infraestrutura do tribunal. Diferentemente das *"options"* e *"packs"* que se incorporam ao *Oracle Database* como extensões de funcionalidade, esta *"appliance"* necessita estar apartada dos servidores de banco de dados, pois atua justamente como uma barreira de segurança impedindo que requisições não autorizadas cheguem ao banco.

No levantamento das contratações públicas similares, apresentado na seção *Contratações similares realizadas pela administração pública*, constata-se a prevalência deste produto Oracle nas aquisições. Não obstante, trata-se de um produto apartado, ao contrário dos demais itens, que são extensões já disponíveis no próprio SGBD Oracle. Ademais, a independência de operação do próprio *Oracle Audit Vault & Database Firewall* em relação ao SGBD do mesmo fabricante se evidencia pelo fato do referido produto suportar outros SGBDs de outros fabricantes.

Deste modo, considerando-se que os requisitos funcionais do grupo AEM podem, em tese, ser atendidos por produtos de mercado concorrentes do *Oracle Audit Vault & Database Firewall,* procedeu-se a pesquisa de mercado a fim de se compararem os produtos compatíveis em análise mais aprofundada, identificados no Quadro 2 adiante, tendo-se adotado, como referência, o relatório independente da publicação digital *PeerSpot*[10] *"Database Security Buyer's Guide & Reviews"* (SEI nº 0004598). Do relatório, foram selecionados, para aprofundamento desta análise, os produtos que receberam as três posições superiores pelo relatório, a saber: *IBM Guardium Data Protection*, *Imperva SecureSphere Database Security* e o próprio *Oracle Audit Vault*.

Quadro 2: Sumário do relatório *"Database Security Buyer's Guide & Reviews"* (SEI nº 0004598), publicado por PeerSpot

Seq.	Fabricante / Produto	Qtde. de avaliações	Governo	Tamanho empresa: 1-200	Tamanho empresa: 201-1000	Tamanho empresa: 1001-	Nota média	Aspectos positivos	Aspectos negativos (necessidade de melhoria)
1	IBM Guardium Data Protection https://www.ibm.com/br-pt/security/data-security/guardium	16	6%	18%	8%	75%	8,3	• Bom desempenho. • Estabilidade e robustez • Facilidade de uso • Fácil implantação • Opções de monitoramento abrangentes. • Alta	• Recursos de firewall inferiores. • Relatórios deficientes. • Suporte técnico ruim. • Configuração inicial de integrações é

Seq.	Fabricante / Produto	Qtde. de avaliações	Governo	Tamanho empresa: 1-200	Tamanho empresa: 201-1000	Tamanho empresa: 1001-	Nota média	Aspectos positivos	Aspectos negativos (necessidade de melhoria)
								confiabilidade. • Licenciamento simples. • Custo favorável.	difícil. • Automação deficiente. • Aprendizado de máquina ausente. • Funcionalidades de análise deficientes.
2	Imperva SecureSphere Database Security https://www.imperva.com/products/data-security/	11	6%	31%	18%	51%	8	• Opções de auditoria granular. • Adequado para atender a diretrizes de *compliance* em privacidade de dados. • Favorece a segurança do acesso aos dados por DBAs. • Preço competitivo*.	• Relatórios deficientes. • Interface de usuário (GUI) antiquada. • Sistema pouco amigável. • Inadequado para ambiente em nuvem. • Suporte técnico ruim. • Desempenho ruim em BDs de uso intenso. • Solução cara*.
3	Oracle Audit Vault and Database Firewall https://www.oracle.com/br/database/technologies/security/audit-vault-firewall.html	3	6%	38%	29%	33%	8,3	• Nível de segurança avançado. • Adequação ao ecossistema Oracle. • Solução escalável.	• Ônus de se manterem dois servidores – um para firewall e outro para auditoria. • Migração entre versões não é simples. • Agrupamento de bancos de dados pode ser melhorada. • Relatórios deficientes. • Carência de funcionalidades disponíveis na solução da Imperva. • Estabilidade deve ser melhorada.

* As avaliações de custo da solução Imperva SecureSphere Database Security são contraditórias. Uma avaliação específica[11] sugere que a política de preços do fabricante mudou com o tempo, tornando-se mais competitiva.

5. Contratações Similares Realizadas pela Administração Pública

Contratações localizadas no ComprasNet[12] , com chave de busca “Oracle Security”.

5.1. Contratação TRE/MA 2021

Órgão contratante:	Tribunal Regional Eleitoral do Maranhão – TRE/MA – UASG: 70005
Procedimento de contratação:	Pregão Eletrônico nº 30/2021 (set. 2021)
URL de referência:	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=70005&modprp=5&numprp=302021
Objeto da contratação:	*Aquisição das seguintes options para segurança de banco de dados Oracle, incluindo os respectivos serviços de atualização e suporte: Oracle Advanced Security - Processor Perpetual; Oracle Data Masking and Subsetting Pack - Processor Perpetual; Oracle Audit Vault and Database.*

Detalhamento do objeto e custo estimado:

Item	Descrição	Qtde.	Vlr. unitário estimado	Subtotal estimado
1	Oracle Advanced Security	4	R$ 114.144,10	R$ 456.576,40

Detalhamento do objeto e custo estimado:				
2	Oracle Data Masking and Subsetting Pack	4	R$ 87.510,53	R$ 350.042,12
3	Oracle Audit Vault and Database Firewall	4	R$ 45.657,54	R$ 182.630,16

5.2. Contratação ETICE 2021

Órgão contratante:	Empresa de Tecnologia da Informação do Ceará – ETICE – UASG: 943001
Procedimento de contratação:	Pregão Eletrônico nº 20210003 / ComprasNet nº 415/2021
URL de referência:	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=943001&modprp=5&numprp=4152021
Objeto da contratação:	*Registro de Preços, visando futuras e eventuais aquisições de licenças e contratações de serviços relacionados à Plataforma Oracle, incluindo suporte técnico e atualização tecnológica pelo período de 12 (doze) meses, a fim de viabilizar a continuidade dos serviços vinculados a estes produtos no ambiente computacional da Empresa de Tecnologia da Informação do Ceará – ETICE e demais órgãos do governo do Estado do Ceará, que fazem uso de serviços técnicos especializados nesta plataforma, de acordo com as especificações e quantitativos previstos no Anexo I – Termo de Referência deste edital.*

Detalhamento do objeto e custo*:

Item	Descrição	Qtde.	Valor unitário	Subtotal
5.	Oracle Database Vault – Licença de uso perpétuo para 1 (um) processador com suporte e atualização de software por 1 (um) ano.	10	R$ 50.556,64	R$ 505.566,40
9.	Oracle Data Masking and Subsetting Pack – Licença de uso perpétuo para 1 (um) processador com suporte e atualização de software por 1 (um) ano.	10	R$ 50.556,64	R$ 505.566,40
13.	Oracle Audit Vault and Database Firewall – Licença de uso perpétuo para 1 (um) processador com suporte e atualização de software por 1 (um) ano.	10	R$ 26.377,38	R$ 263.773,80
15.	Oracle Advanced Security – – Licença de uso perpétuo para 1 (um) processador com suporte e atualização de software por 1 (um) ano.	10	R$ 65.943,44	R$ 659.434,40
20.	Serviço de consultoria de operação assistida incluindo apoio de especialistas em soluções Oracle para instalação, configuração, administração, treinamento e serviços de nuvem relacionados com as soluções contratadas.	5000	R$ 150,91	R$ 754.550,00
Total da contratação dos itens:			**R$ 193.434,10¤**	**R$ 2.688.891,00**

* Fonte: https://s2gpr.sefaz.ce.gov.br/licita-web/paginas/licita/PublicacaoList.seam

¤ Total unitário de um conjunto de todos os itens, calculado como referência unitária geral do valor da contratação.

5.3 Contratação CJF DF 2019

Órgão contratante: Secretaria do Conselho da Justiça Federal – CJF-DF UASG: 90026

Procedimento de contratação: Pregão Eletrônico nº 29/2019 (nov. 2019)

URL de referência: http://www.comprasnet.gov.br/consultalicitacoes/download/download_editais_detalhe.asp?coduasg=90026&modprp=5&numprp=292019

Objeto da contratação: *Aquisição de licenças de uso perpétuo e ilimitado (por 12 meses), na modalidade Acordo de Licenciamento Ilimitado (Unlimited License Agreement – ULA), de softwares Oracle.*

Detalhamento do objeto e custo:

Item	Descrição	Qtde.	Vlr. unitário estimado	Subtotal estimado
8.	Oracle Advanced Security - Processor Perpetual Ilimitada	ilimitada	O edital da licitação apresenta apenas um valor estimado global para toda a contratação – R$ 5.351.187,23 – a qual inclui outros itens além daqueles previstos no presente estudo, inviabilizando se determinar o valor unitário.	
9.	Oracle Database Vault - Processor Perpetual Ilimitada			
11.	Oracle Data Masking and Subsetting - Processor Perpetual Ilimitada			

5.4 Contratação IBAMA 2018

Órgão contratante: Ministério do Meio Ambiente – UASG: 193099

Procedimento de contratação: Pregão Eletrônico nº 23/2018 (out. 2018)

URL de referência: http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=193099&modprp=5&numprp=232018

Objeto da contratação: *Registro de preços para contratação de empresa especializada para o fornecimento de Produtos (Hardware e Software) da Plataforma Oracle, com suporte técnico e atualização tecnológica pelo período de 12 (doze) meses para viabilizar a continuidade dos serviços vinculados a estes produtos no ambiente computacional do IBAMA, bem como a prestação de serviços técnicos especializados nesta plataforma e nas tecnologias Oracle, de acordo com as especificações e quantitativos estimados constantes do Termo de Referência (Anexo I) deste Edital.*

Detalhamento do objeto e custo estimado:

Item	Descrição	Qtde.	Vlr. unitário estimado	Subtotal estimado
6.	Oracle Data Masking	8	R$ 47.381,04	R$ 379.048,32
7.	Oracle Advanced Security	8	R$ 65.778,02	R$ 526.224,16
11.	Fornecimento de Serviços Especializados de Instalação, Configuração, Suporte Remoto / Manutenção, Evolução Tecnológica e treinamentos para Banco de Dados e Aplicações Oracle.	4800	R$ 588,33	R$ 2.823.984,00

5.5 Contratação ETICE 2017

Órgão contratante: Empresa de Tecnologia da Informação do Ceará – ETICE UASG: 943001

Procedimento de contratação: Pregão Eletrônico nº 1365/2017 (dez. 2017)

URL de referência: http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=943001&modprp=5&numprp=13652017

Objeto da contratação: *Registro de Preço para futuros e eventuais aquisições de Produtos de Hardware e Software da Plataforma Oracle para atendimento à Empresa de Tecnologia da Informação do Ceará, bem como a prestação de serviços técnicos nesta Plataforma, de acordo com as especificações e quantitativos estimados constantes, de acordo com as especificações e quantitativos previstos no Anexo I – Termo de Referência deste edital.*

Detalhamento do objeto e custo*:

Item	Descrição	Qtde.	Vlr. unit. contratado	Subtotal contratado
6.	Oracle Advanced Security	24	R$ 59.999,00	R$ 1.439.976,00
7.	Oracle Database Vault	24	R$ 44.999,99	R$ 1.079.999,76
10.	Oracle Data Masking and Subsetting	24	R$ 44.999,99	R$ 1.079.999,76
17.	Oracle Audit Vault and Database Firewall	24	R$ 22.999,99	R$ 551.999,76
36.	Serviço de consultoria de operação assistida incluindo apoio de especialistas em soluções da Oracle para instalação, configuração, administração, treinamento e serviços de nuvem relacionados com as soluções contratadas.	25000	R$ 495,00	R$ 12.375.000,00
Total da contratação dos itens:			**R$ 172.998,97¤**	**R$ 16.526.975,28**

* Fonte: https://s2gpr.sefaz.ce.gov.br/licita-web/paginas/licita/PublicacaoList.seam

¤ Total unitário de um conjunto de todos os itens, calculado como referência unitária geral do valor da contratação.

5.6 Contratação IN 2017

Órgão contratante: Fundo de Imprensa Nacional – UASG: 110245

Procedimento de contratação: Pregão Eletrônico nº 1/2017 (jan. 2017)

URL de referência: http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=110245&modprp=5&numprp=12017

Objeto da contratação: *Registro de Preços para contratação de empresa para fornecimento de licença de uso de produtos Oracle, incluindo atualização de versões, serviços de suporte técnico e consultoria, sob demanda na modalidade de Unidade de Suporte Técnico - UST, conforme especificações constantes do Termo de Referência - Anexo I deste edital.*

Detalhamento do objeto e custo*:				
Item	**Descrição**	**Qtde.**	**Vlr. unitário estimado**	**Subtotal estimado**
6.	Oracle Database Vault	22	Não disponível. Valores estimados não constam no edital obtido no ComprasNet e Contrato nº 08/2017*, resultante da ARP, encontrado, não contempla os referidos itens.	
7.	Oracle Audit Vault	20		
8.	Oracle Advanced Security	22		
13.	Serviço de consultoria para instalação, criação de ambiente, migração, integração, acompanhamento e transferência de tecnologia – sob demanda em Unidade de Suporte Técnico – UST.	550	R$ 336,59	R$ 185.124,50

* Contrato nº 08/2017, entre a Imprensa Nacional e a empresa Magna Sistemas Consultoria S.A. Disponível em: https://www.in.gov.br/documents/49035737/49284645/contrato_08_2017___magna_sistemas.pdf/3a3ac27c-3989-4a86-9b3b-3ce27e41a8be. Acesso em 25/05/2022.

5.7 Acordo Corporativo nº 10/2021 – Catálogo de Soluções de TIC - ORACLE

> *"Os Catálogos de Soluções de TIC com Condições Padronizadas são instrumentos previstos na Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, com redação dada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019.*
>
> *Trata-se de uma relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço, Preço Máximo de Compra de Item de TIC (PMC-TIC), entre outros elementos.*
>
> *(...)*
>
> *Os Catálogos de Soluções de TIC com Condições Padronizadas são elaborados a partir da identificação das soluções de TIC de uso mais difundido no âmbito da Administração Pública Federal. Em seguida, analisa-se a materialidade das contratações dessas soluções, considerando os órgãos SISP e os não-SISP e o período mínimo de 3 anos anteriores à análise. A partir dessas informações, a Secretaria de Governo Digital estabelece as condições padrões para a aquisição dessas soluções de TIC, incluindo os seus respectivos PMC-TIC, calculados considerando os preços praticados no âmbito da Administração Pública.*
>
> *Os Catálogos podem ser construídos por meio de processo de negociação com o fabricante da solução, ou publicados unilateralmente pela Secretaria de Governo Digital, a partir de dados oriundos de contratações feitas no âmbito do SISP, pesquisas de mercado, além de outros elementos."*

Fonte: Governo Digital[13]

O Acordo Corporativo nº 10/2022 (SEI nº 0004819)[14] , mantido entre o fabricante ORACLE e o Governo Federal, estabelece, em seu ANEXO I (SEI nº 0004829) o Catálogo de Soluções de TIC[15] daquele fabricante, incluindo, além da relação de produtos, as condições e preços padronizados praticados pelo fabricante junto às instituições de governo aderentes ao acordo. Incluem-se nos autos o ANEXO II ao referido acordo, que apresenta a Minuta do Termo de Adesão (SEI nº 0004835). Por fim, verifica-se que o Acordo Corporativo nº 10/2021 encontra-se vigente por mais 12 meses a partir de 15/07/2022, conforme seu segundo aditivo (SEI nº 0004826).

Dentre os órgãos da Justiça Eleitoral, dentre as instituições aderentes ao Acordo nº 10/2021, consta o Tribunal Regional Eleitoral de Minas Gerais (TRE/MG)[16] .

Quadro 3: Preços padronizados do Acordo nº 10/2021, entre a União e a ORACLE

Item	**Descrição**	**PMC-TIC**	**Qtde. referencial (TRe de nível médio)**	**Subtotais**
OR-007	Oracle Advanced Security	R$ 77.231,50	4	R$ 308.926,00
OR-008	Oracle Data Masking and Subsetting	R$ 59.210,82	4	R$ 236.843,28
OR-009	Audit Vault and Database Firewall	R$ 30.892,60	4	R$ 123.570,40
OR-010	Oracle Database Vault	R$ 59.210,82	4	R$ 236.843,28
			Estimativa Total da Contratação (referencial):	**R$ 906.182,96**

Item	Descrição	PMC-TIC	Qtde. referencial (TRe de nível médio)	Subtotais
Para todos os itens, considere-se:				

Categoria: Plataforma de dados.

Modelo de licenciamento: Licença Perpétua + Suporte e Atualização (SA).

Vigência SA: 12 (doze) meses.

---

6. Estratégia para a Contratação

6.1. Indicação e Caracterização da Solução Escolhida

O presente estudo conclui pela necessidade de separação em duas contratações. Em ambas, deve ser adotado o Sistema de Registro de Preços, de forma a permitir que os Tribunais Participantes planejem e definam prioridades, realizando sua contratação conforme seus próprios critérios de oportunidade e conveniência. A adesão de órgãos não participantes à Ata de Registro de Preços resultante desta contratação deve se limitar aos tribunais eleitorais -- TSE e TREs. Justifica-se a permissão de adesão à ARP pelos tribunais eleitorais por se tratar, a presente aquisição, de iniciativa vinculada ao Programa nacional de Cibersegurança da Justiça Eleitoral, o qual todos os tribunais eleitorais integram.

A primeira contratação compreende a ativação do licenciamento de itens de software já presentes dentro do SGBD Oracle Enterprise, a saber:

a. *Oracle Advanced Security*
b. *Oracle Data Masking and Subsetting Pack*
c. *Oracle Database Vault*

Conforme explicado na seção *Análise das Soluções de Mercado*, estes itens compreendem funcionalidades já existentes no SGBD Oracle instalado nos ambientes dos tribunais participantes, e atendem aos requisitos de criptografia de dados (CRP), reescrita de dados (RES), mascaramento e seleção de subconjunto de dados (MSK) e controle de acesso (CAC). Por serem programas distribuídos em conjunto com o produto de software Oracle Database Enterprise Edition – já estando, portanto, instalados na infraestrutura tecnológica dos tribunais participantes – são denominados, pelo fabricante, de *"options"* e *"packs"* porque são opcionais de segurança que estendem as funcionalidades de segurança do banco Oracle e requerem a aquisição de licenças específicas de uso, embora a distribuição esteja diretamente vinculada ao produto Oracle Database. Portanto, considerando o reduzido risco de incompatibilidade entre os produtos e também com o banco de dados, a simplicidade de instalação e manutenção, a atuação como verdadeiras extensões de funcionalidade.

Informações adicionais:

a. Fornecedor: Existem dezenas de parceiros de revenda de licenças no Brasil[17] , dos quais enumeram-se no *Anexo A* aqueles que atendem o setor público.
b. Entidade proprietária da solução: Oracle.
c. Estimativa de Orçamento: R$ 24.095.291.49, conforme *Anexo C - Estimativa de Preços*.
d. Aderência da Solução ao MNI, ao ICP-Brasil e ao Moreq-Jus: Não se aplica.

A segunda contratação visa o atendimento dos requisitos de auditoria de atividades e monitoramento de instruções no banco de dados (AEM). Tendo se constatado que o produto da Oracle – o Oracle Audit Vault & Database Firewall – usualmente adquirido para este fim, diferentemente dos demais produtos, trata-se de um produto em separado, vendido como *software appliance*, além da existência de produtos concorrentes com funcionalidade similares, entende-se que uma contratação específica deve ser realizada para atender estes requisitos, em separada da primeira, por se considerar, também:

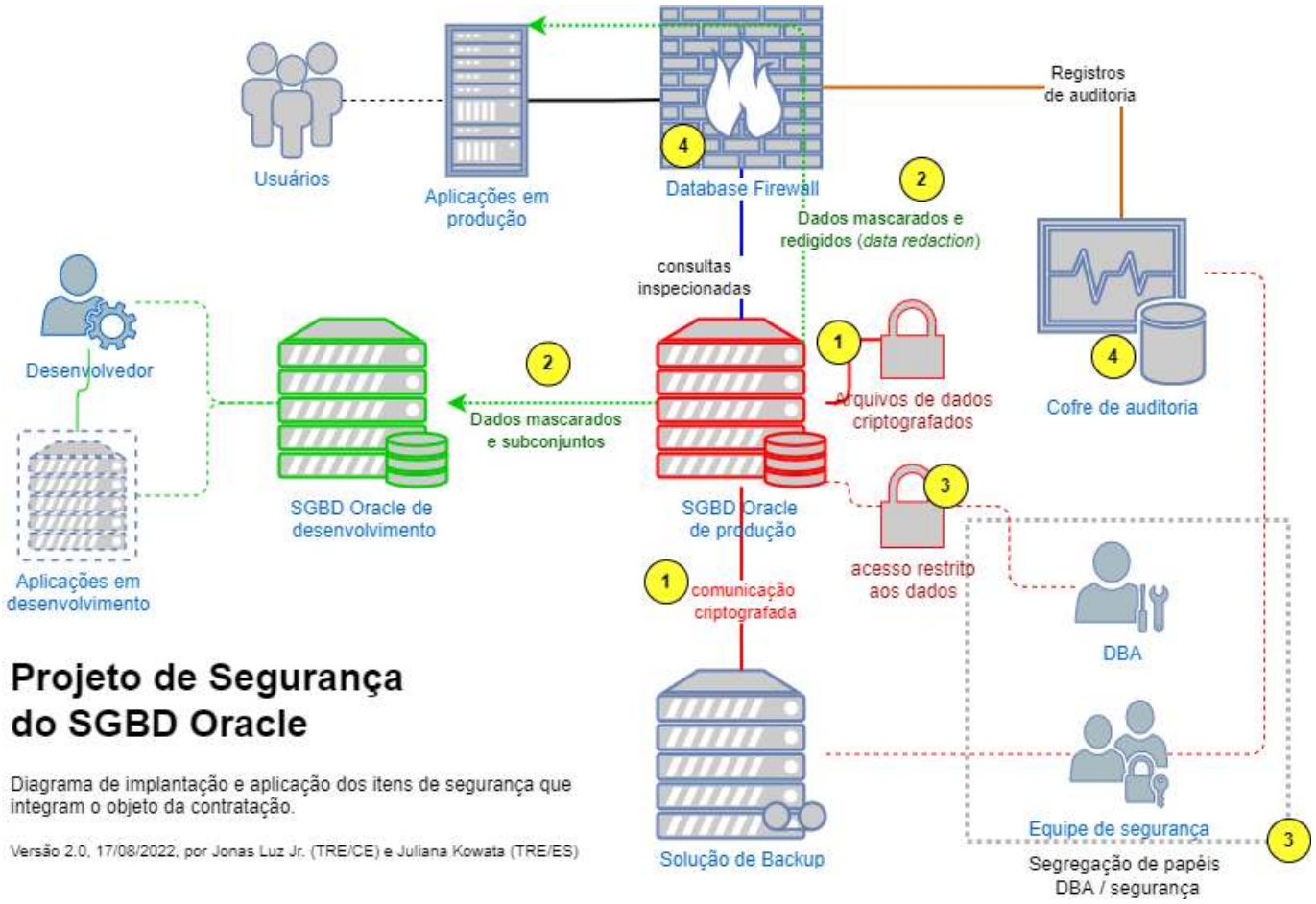
a. Esta contratação irá requerer a realização de prova de conceito, de forma a garantir que a solução a ser contratada cumpra precisamente com os requisitos especificados no Termo de Referência;
b. Uma vez que poderá ser adquirido produto de mercado com o qual as equipes técnicas dos tribunais participantes não tenham experiência ou conhecimento técnico, esta contratação deverá conter item de

prestação de serviço, repasse tecnológico ou treinamento. Estes itens, por sua interdependência, deverão ser contratados em lote.

Compõe a segunda contratação:

a. Solução de software de auditoria e firewall de banco de dados;
b. Serviço de consultoria de operação assistida incluindo apoio de especialistas para instalação, configuração e administração, relacionados com a solução contratada.
c. Treinamento oficial do fabricante com duração de, pelo menos, 40 horas, para equipe de 8 pessoas.

Por fim, apresenta-se na figura abaixo (SEI nº 0003915), o diagrama de implantação das soluções a serem contratadas e sua integração.



6.2. Justificativa da Escolha da STIC

A divisão da presente demanda em duas contratações é recomendada por se verificar que:

1. No caso dos itens 1 a 3, verifica-se vantajosidade no atendimento à demanda por meio de licenciamento das extensões de funcionalidade já disponíveis no próprio SGBD, a partir dos critérios e benefícios dessa contratação, elencados na seção *"Análise das soluções de mercado para a demanda"*, notadamente: aderência à padronização do ambiente de desenvolvimento e operação dos bancos de dados na Justiça Eleitoral e risco praticamente nulo de incompatibilidade dos produtos com o SGBD alvo da contratação, associados, secundariamente, aos critérios de simplicidade de instalação e manutenção. Em se tratando de produtos de segurança nativos para o Oracle Database EE, observam-se as seguintes implicações:

    a. Garantia de suporte e compatibilidade entre as versões dos produtos de segurança e a do banco de dados, pois observam a arquitetura do banco de dados Oracle e acompanham calendário do ciclo de vida;
    b. Minimização de sobrecarga decorrente de integração entre diferentes produtos, pois se integram aos recursos de forma nativa, atuando como verdadeiras extensões de funcionalidade do Oracle Database Enterprise Edition;
    c. Redução do impacto cultural, uma vez os produtos observam concepção e conceitos da arquitetura Oracle com a qual a equipe técnica está ambientada;

d. Redução de necessidade de intervenção no ambiente tecnológico, considerando que alguns dos produtos já se encontram instalados e acessíveis para uso;

e. Reconhecimento automático das extensões de segurança pelas interfaces de administração do Oracle Database que são utilizadas pelas equipes técnicas.

2. No caso do quarto item – "Solução de auditoria e firewall de banco de dados" –, constata-se, nas contratações similares identificadas, a prevalência do produto *Oracle Audit Vault & Database Firewall.* Não obstante, o referido produto, diferentemente daqueles elencados anteriormente, trata-se de um produto independente do próprio SGBD, servindo inclusive a SGBDs de outros fabricantes e, possuindo concorrência de mercado de produtos com mesma finalidade e também compatíveis com Oracle.

6.3. Análise da Dependência Tecnológica

O Oracle Database é um sistema de gerenciamento de banco de dados ao qual parte significativa das soluções da Justiça Eleitoral é estruturalmente acoplada, gerando estreita dependência tecnológica das soluções ao produto.

A adoção do Oracle Database tornou-se mandatória – como um padrão *de facto* – para os Tribunais Regionais Eleitorais, a julgar 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 nos tribunais participantes.

Portanto, a indicação de contratação de uma solução de TIC cujos componentes são integrados nativamente ao ambiente do Oracle Database não altera a dependência tecnológica já existente.

6.4. Descrição da Solução e Sua Relação com a Demanda Prevista

6.4.1. Contratação/Lote nº 1

LOTE/CONTRATAÇÃO 1 – *Options/Packs* do SGBD *Oracle Enterprise Edition* – CATMAT/CATSER: 27464

Item	Descrição	Métrica①	Unidade de Medida①	Qtde. Geral Estimada②	Vlr. unit. estimado③	Subtotal estimado
1	Oracle Advanced Security – Licença de perpétuo com suporte e atualização de software por 12 meses	processador	unidade	104	R$ 69.650,99	R$ 7.243.702,96
2	Oracle Data Masking and Subsetting Pack – Licença de perpétuo com suporte e atualização de software por 12 meses	processador	unidade	96	R$ 52.382,83	R$ 5.028.751,68
3	Oracle Database Vault – Licença de perpétuo com suporte e atualização	processador	unidade	112	R$ 51.589,15	R$ 5.777.984,80

LOTE/CONTRATAÇÃO 1 – *Options/Packs* do SGBD *Oracle Enterprise Edition* – CATMAT/CATSER: 27464

	de software por por 12 meses			

Total Geral Estimado do Lote/Contratação: R$ 18.050.439,44

Adjudicação: Menor preço por item

① Vide *Anexo E - Memória de Cálculo*.
② Quantidade estimada a partir do levantamento de demanda realizado junto aos Tribunais Participantes (*Anexo B*).
③ Valor unitário estimado a partir das contratações públicas identificadas (seção "Contratações Similares Realizadas pela Administração Pública" , *Anexo C*).

Justificativa da adjudicação: A adjudicação por item se justifica pela simplicidade e independência do fornecimento, uma vez que são produtos padronizados do fabricante.

6.4.2. Contratação/Lote nº 2

LOTE/CONTRATAÇÃO 2 – Produto de Firewall e Auditoria para banco de dados

Item	Descrição	Qtde. Geral Estimada	Vlr. unit. estimado	Subtotal estimado
1	Solução de software de auditoria e firewall de banco de dados	128 ①	R$ 26.756,66 ③	R$ 3.424.852,05
2	Serviço de consultoria de operação assistida incluindo apoio de especialistas para instalação, configuração e administração, relacionados com a solução contratada.	8000 ②	R$ 327,50 ④	R$ 2.620.000,00
3	Treinamento oficial do fabricante com duração de, pelo menos, 40 horas, para equipe de 8 pessoas.	20 ③	N/D ⑤	N/D ⑤

Subtotal estimado do lote/contratação: R$ 6.044.852,05

Adjudicação: Menor preço total do lote

① Quantidade estimada a partir do levantamento de demanda realizado junto aos Tribunais Participantes (*Anexo B*), com base na forma de licenciamento do produto Oracle Database Audit Vault & Database Firewall.
② Quantidade estimada a partir do levantamento de demanda realizado junto aos Tribunais Participantes (*Anexo B*), considerando 400 horas de serviço por tribunal (20 tribunais).
③ Valor unitário estimado a partir das contratações públicas identificadas (seção E, *Anexo C*), com base no produto Oracle Database Audit Vault & Database Firewall.
④ Valor unitário estimado a partir das contratações públicas identificadas (seção E , *Anexo C*).
⑤ Não disponível. O valor de referência do Termo de Referência deverá se basear em pesquisa de preços junto ao mercado.

Justificativa da adjudicação: A adjudicação por lote se justifica pela interdependência dos itens do lote e sua entrega.

6.5. Indicação da Necessidade de Adequação Ambiental

Item	Descrição	Necessidade de Adequação Ambiental
1	Oracle Advanced Security	Configuração de cofre para chaves Não serão necessários recursos adicionais de hardware.
2	Oracle Data Masking and Subsetting Pack	Não serão necessários recursos adicionais de hardware.
3	Oracle Database Vault	Não serão necessários recursos adicionais de hardware.
4	Solução de software de auditoria e firewall de banco de dados. ①	Ambiente de Virtualização Requisitos de Memória: cada servidor x86 64-bit deve ter minimamente: • Audit Vault Server: 8 GB • Database Firewall: 8 GB Requisitos de Espaço: cada servidor x86 64-bit deve ter um único hard drive com o mínimo descrito a seguir: • Audit Vault Server: 220 GB • Database Firewall: 220 GB

① Critérios baseados no produto de referência Oracle Audit Vault & Database Firewall. Fonte: https://docs.oracle.com/en/database/oracle/audit-vault-database-firewall/20/sigig/preinstall.html#GUID-8539DA7B-9C51-493F-AE92-5CEC551D1221.

7. Análise de Riscos

Obrigatório para as contratações ou prorrogações, cuja estimativa de preços seja igual ou superior ao valor disposto no art. 23, inciso II, alínea "a", da Lei nº 8.666/93.

7.1. Análise de Riscos e Estratégias de Mitigação

7.1.1. Identificação e Análise de Riscos

RISCO 1	**Uso inadequado/insuficiente da solução de TIC**	
Probabilidade ***(Alta, média ou baixa)***	Alta	
	Efeito (Dano)	**Impacto** ***(Baixo, Médio ou Alto)***
1	Uso inadequado da solução de TIC pode ocasionar impactos no desempenho dos bancos gerenciados ou perda de dados.	Médio
	Ações de Mitigação e Contingência	**Responsável**
1	Viabilizar capacitação	Coordenadorias de Infraestrutura de TIC
2	Definir papéis e responsabilidades no uso da solução de TIC	Seções de Banco de Dados
3	Elaborar plano de implantação da solução de TI	Coordenadorias de Infraestrutura de TIC Seções de Banco de Dados

RISCO 2	**Obsolescência da solução de TIC decorrente de fim de vigência contratual de atualização e suporte**	
Probabilidade ***(Alta, média ou baixa)***	Alta	
	Efeito (Dano)	**Impacto** ***(Baixo, Médio ou Alto)***
1	Perda de efetividade no uso da solução de TIC decorrente de obsolescência	Alto
	Ações de Mitigação e Contingência	**Responsável**
1	Avaliar periodicidade para renovação de contrato de suporte	Coordenadorias de Infraestrutura de TIC
2	Definir rotina para atualização de solução durante vigência contratual	Seções de Banco de Dados
3	Acompanhar vigência contratual	Gestores contratuais

RISCO 3	**Ausência de recursos financeiros para custeio da renovação anual dos serviços de atualização e suporte**	
Probabilidade ***(Alta, média ou baixa)***	Alta	
	Efeito (Dano)	**Impacto** ***(Baixo, Médio ou Alto)***
1	Perda de efetividade no uso da solução de TIC decorrente de obsolescência	Alto
2	Impedimento de atualização do Oracle Database	Alto
	Ações de Mitigação e Contingência	**Responsável**
1	Avaliar periodicidade para renovação de contrato de suporte	Coordenadorias de Infraestrutura de TIC
2	Definir rotina para atualização de solução durante vigência contratual	Seções de Banco de Dados
3	Acompanhar vigência contratual	Gestores contratuais

RISCO 4	**Incapacidade de implantação da solução de TIC em sua**

	completude em decorrência de demandas sazonais prioritárias próprias de anos eleitorais	
Probabilidade (Alta, média ou baixa)	Alta	
	Efeito (Dano)	**Impacto *(Baixo, Médio ou Alto)***
1	Contratação da solução de TIC	Alto
	Ações de Mitigação e Contingência	**Responsável**
1	Elaborar plano de implantação considerando recursos humanos, materiais e o fator do "ano eleitoral"	Coordenadorias de Infraestrutura de TIC
2	Privilegiar a contratação fatiada da solução de TIC, na forma de Ata de Registro de Preço, de modo a realizar o empenho financeiro casado com o plano de implantação.	Equipe de Contratação

RISCO 5	**Sobreposição de responsabilidade no uso da solução de TIC entre a equipe de segurança cibernética, de banco de dados e de sistemas operacionais**	
Probabilidade (Alta, média ou baixa)	Alta	
	Efeito (Dano)	**Impacto *(Baixo, Médio ou Alto)***
1	Conflito de responsabilidades e sobreposição de funcionalidades com outras iniciativas de aquisição de produtos de segurança.	Alto
	Ações de Mitigação e Contingência	**Responsável**
1	Elaborar plano de implantação considerando responsabilidades de cada equipe.	Coordenadorias de Infraestrutura de TIC
2	Comunicar equipes envolvidas sobre as funcionalidades da solução de TIC para que se manifestem sobre a existência ou não de iniciativas de aquisição similares.	Equipe de Contratação Coordenadorias de Infraestrutura de TIC

7.2. Descontinuidade do Fornecimento

As licenças dos produtos de software desta contratação tem o caráter de serem perpétuas, ou seja, uma vez adquiridas, não haverá o impedimento de uso. Entretanto, o serviço de suporte técnico e a possibilidade de atualização de versão da solução de TIC podem ser prejudicados na ocorrência de descontinuidade do fornecimento.

Ocorre que, havendo a descontinuidade do produto, as atualizações de versão da STIC não mais ocorrerão, resultando, em poucos anos, na obsolescência da tecnologia e em riscos à segurança do ambiente tecnológico. Como atenuante está o fato de que produtos da Oracle possuem previsibilidade de descontinuidade de fornecimento em decorrência de calendários de ciclo de vida divulgados com antecedência suficiente para que providências e estudos adaptativos sejam conduzidos.

Entretanto, a equipe técnica deve, no exercício de suas funções, manter os produtos atualizados ao longo da vigência contratual, a fim de que o ambiente acompanhe a evolução das versões, mantendo a mais recente, de forma a contornar o imponderável da descontinuidade não programada de um ou mais produtos de software que compõem a solução de TIC. Neste sentido, devem os Tribunais Contratantes ficarem cientes da necessidade de manutenção de contrato continuado, renovável anualmente ou pelo período permitido em lei, de atualização e suporte técnico das soluções de software contratadas, evitando, assim, a descontinuidade do serviço.

Em se configurando a descontinuidade dos produtos, há alternativas:

a. Migrar para a solução de TIC que substituiu a solução descontinuada;

b. Desabilitar os mecanismos de segurança, sem prejuízo ao banco de dados;

c. Manter os mecanismos de segurança, com o efeito colateral de impedir as atualizações de versão do Oracle Database da contratante.

8. Análise de Sustentação do Contrato

Obrigatório para as contratações ou prorrogações, cuja estimativa de preços seja igual ou superior ao valor disposto no art. 23, inciso II, alínea "a", da Lei nº 8.666/93.

8.1. Da Renovação de Licenças da STIC

Após o período de 12 (doze) meses do início da vigência contratual, findar-se-ão os acessos aos serviços de suporte técnico e de atualização da solução de TIC. O reestabelecimento do acesso aos serviços citados demandará por nova contratação, conduzida anualmente, cujo custo estimado é de aproximadamente 22% (vinte de dois por cento) do custo da presente contratação, conforme informações do fabricante[18] .

8.2. Das Medidas de Preservação de Investimento

Medidas para preservar o investimento incluem:

a. Definir processo para gerenciar licenças da solução de TIC, de forma a impedir o uso de superior ao quantitativo adquirido;
b. Definir processo para atualização de solução de TIC enquanto vigorar o contrato;
c. Definir estratégia de uso adequado da solução de TIC, a fim de adequar aos diferentes perfis de atuação das equipes de Banco de Dados e das equipes de Segurança da Informação.

8.3. Recursos Materiais e Humanos

8.3.1. Recursos Materiais

Adicionalmente aos recursos materiais descritos na seção *Indicação da Necessidade de Adequação Ambiental*, devem ser considerados:

a. Plano de capacitação contínua da equipe;
b. Plano de implantação da solução de TIC.

8.3.2. Recursos Humanos

a. Alocação de equipe capacitada e dedicada à implantação e uso da solução de TIC;
b. Alocação de equipe capacitada e dedicada ao uso da solução de TIC;
c. Alocação de gerente de projetos para a implantação da solução de TIC.

ANEXO A – LISTA DE POTENCIAIS FORNECEDORES

Relação de Fornecedores ORACLE autorizados para venda com o Setor Público. Fonte: fabricante, por EMAIL (SEI nº 0007921)

Seq.	Fornecedor	Contato
1	Accenture do Brasil Ltda.	Sítio: https://www.accenture.com/br-pt/about/contact-us Telefone: (11) 5188-3000 Email: patricia.costa.nunes@accenture.com
2	Accerte Tecnologia Da Informacao Ltda-epp	Sítio: https://accerte.com.br/contato/ Telefone: (62) 3945-9510 Email: licitacoes@accerte.com.br
3	Advanced Database & IT Sistemas De Informacao S A	Sítio: https://www.advancedit.com.br/sobre/ Telefone: (11) 4118-0486 Email: comercial@advancedit.com.br
4	Ax4b Sistemas De Informatica Ltda	Sítio: https://ax4b.com/contato/ Telefone:(11) 98845-0931 Email: Romulo.oliveira@ax4b.com
5	Bb Tecnologia E Servicos S.A	Sítio: https://bbts.com.br/index.php/form-fale-conosco Telefone:(61) 4003-7809 Email: comercial@bbts.com.br
6	Capgemini Brasil S.A.	Email: vendaspublic.br@capgemini.com
7	Centurylink Comunicações do Brasil Ltda	Sítio: https://www.lumen.com/pt-br/contact-us.html Telefone: (11) 98817-6283 (whatsapp) Email: contato.br@lumen.com
8	Compethics It Solucoes Em Tecnologia Da Informacao Eireli	Sítio: https://compethics.com.br/contato Telefone: (51) 99819-3043 Email: alexandre_piano@lta-rh.com.br
9	Compwire Informatica S/A	Sítio: https://www.compwire.com.br/contato Telefone: (41) 3333.6066 Email: contato@compwire.com.br
10	CSI Centro de Soluções em Informática Ltda. / CSI Inovacao Em Ti Eireli	Sítio: https://csiway.com.br/contato.php Telefone: (27) 99962-7372 Email: almir.carone@csiway.com.br
11	Finality Consultores Associados Ltda.	
12	First Decision Tecnologias Inovadoras E Informatica Ltda	Sítio: https://www.firstdecision.com.br/contato Telefone: (61) 3361-5160 Email: juliano.korff@firstdecision.com.br
13	Halbar Solucoes Em Tecnologia Da Informacao Eireli	Email: alexandre_piano@lta-rh.com.br
14	IT-One Tecnologia Da Informacao S.A.	Sítio: https://itone.com.br/ Telefone: (11) 4003-3716 Email: edgar.luiz@itone.com.br
15	Lanlink Soluções e Comercialização em Informática S/A	Sítio: https://www.lanlink.com.br/ Telefone: (11) 4007-2559 Email: kleper.Porto@lanlink.com.br
16	LTA-RH Informática, Comércio, Representações Ltda.	Sítio: https://www.lta-rh.com.br/ Telefone: (51) 3382-7700 Email: alexandre_piano@lta-rh.com.br
17	MD Serviços de Tecnologia da Informação Ltda.	Email: marcel.carvalho@lustrabits.com.br
18	NEC Latin America S.A.	Sítio: https://contact.nec.com/http-br.nec.com_tb_root_contact/ Telefone: (11) 2166-2300 Email: eduardr@nec.com.br
19	Netmanagement Informática Ltda - EPP (DataCentrics)	Sítio: https://datacentrics.com.br/ Telefone: (51) 3021-0300 Email: licitacoes@datacentrics.com.br
20	Salux - Informatização Em Saúde - S.A	
21	Service Informática Ltda.	Sítio: https://service.com.br/ Telefone: (11) 2595-1400 Email: contato@service.com.br
22	Sumauma Computadores E Telecomunicacoes Ltda	Sítio: http://www.sumaumatelecom.com.br/ Telefone: (11) 3966-2454 Email: tatiana@sumaumatelecom.com.br
23	Tarea Gerenciamento Ltda	Email: comercial@tarea.com.br

Seq.	Fornecedor	Contato
24	Tecnocomp Tecnologia E Servicos Ltda	Sítio: https://www.tecnocomp.com.br/ Telefone: (11) 2199-5800 Email: mauro.marsura@tecnocomp.com.br
25	TLD Teledata Tecnologia em Conectividade Eireli	Sítio: https://www.tld.com.br/teledata/ Telefone: 0800 000 0594 Email: comercial.gov@teledatabrasl.com.br
26	To Brasil Consultoria Em Tecnologia Da Informacao Ltda	Sítio: https://www.to-brasil.com/ Telefone: (11) 3262-2138 Email: giorgio.bottin@to-brasil.com
27	V2 Tecnologia Ltda	Sítio: https://v2com.com/ Telefone: (11) 3031-3322 Email: comercial@v2com.com
28	V8 Consulting Ltda	Sítio: https://www.v8consulting.com.br/ Telefone: (11) 2384-1083 Email: comercial@v8consulting.com.br
29	Verano Engenharia Comercio Importacao E Exportacao Ltda	
30	VS DATA Comércio & Distribuição Ltda.	Sítio: https://vsdata.com.br/fale-conosco/ Telefone: (41) 2118-7035 Email: governo@vsdata.com.br
31	Wipro Do Brasil Sistemas De Informatica Ltda. / Wipro Do Brasil Tecnologia Ltda.	Sítio: https://www.wipro.com/pt-BR/ Telefone: - Email: rodrigo.reis2@wipro.com
32	WISE DATABASE Soluções em TI Ltda - ME	Email: fernando.vilarim@wisedb.com.br

ANEXO B – RELAÇÃO DE TRIBUNAIS PARTICIPANTES

Tribunal participante	Qtde. Estimada – Lote 1 – Item 1 Oracle Advanced Security	Qtde. Estimada – Lote 1 – Item 2 Oracle Data Masking and Subsetting Pack	Qtde. Estimada – Lote 1 – Item 3 Oracle Database Vault	Qtde. Estimada – Lote 2 – Item 1 Solução de Auditoria e Firewall de BD
Totais:	**104**	**96**	**112**	**128**
TRE-AC	4	4	4	4
TRE-AL	4	4	4	4
TRE-AP	4	4	4	4
TRE-DF	8	8	8	8
TRE-GO	8	8	8	8
TRE-PI	4	4	4	4
TRE-RJ	0	0	8	8
TRE-RN	8	0	8	0
TRE/BA	16	16	16	16
TRE/CE	4	4	4	4
TRE/ES	4	4	4	4
TRE/MA	0	0	4	4
TRE/MS	4	4	4	4
TRE/PA	4	4	4	4
TRE/PB	4	4	4	4
TRE/PR	4	4	4	0
TRE/SC	4	4	0	4
TRE/SP	12	12	12	12
TRE/TO	8	8	8	8
TSE	0	0	0	24

ANEXO C – ESTIMATIVA DE PREÇOS

As contratações levantadas na seção *"Contratações Similares Realizadas pela Administração Pública"* foram adotadas como referência para a estimativa do custo da presente contratação, pautando-se pelos seguintes critérios:

a. Foram considerados, pelo menos, três valores para cada item da contratação. Acima disso, foram desprezados, nesta ordem, o maior valor e, em seguida, o menor valor;

b. Das contratações remanescentes, foi obtida a média dos valores para cada item, o que é adotado como o custo médio estimado para a contratação.

O Quadro 4 apresenta os resultados da análise.

Quadro 4 - Estimativa de custo da contratação

Contratação	Advanced Security	Data Masking and Subsetting	Database Vault	Audit Vault & DB Firewall ⑤	Serviço – Repasse tecnológico
Qtde. Geral Estimada da Demanda ①	104	96	112	128	8000
Acordo Corporativo nº 10/2021	R$ 77.231,50	R$ 59.210,82	R$ 59.210,82	R$ 30.892,60	N/D
~~**TRE/MA 2021**~~②	~~R$ 114.144,10~~	~~R$ 87.510,53~~	N/D	~~R$ 45.657,54~~	N/D
ETICE 2021	R$ 65.943,44	R$ 50.556,64	R$ 50.556,64	R$ 26.377,38	R$ 150,91
IBAMA 2018	R$ 65.778,02	R$ 47.381,04	N/D	N/D	~~R$ 588,33~~
IN 2017	N/D	N/D	N/D	N/D	R$ 336,59
~~**ETICE 2017**~~	~~R$ 59.999,00~~	~~R$ 44.999,99~~	R$ 44.999,99	R$ 22.999,99	R$ 495,00
Valores unitários estimados da contratação ③ **(média dos valores válidos)**	**R$ 69.650,99**	**R$ 52.382,83**	**R$ 51.589,15**	**R$ 26.756,66**	**R$ 327,50**
Subtotais estimados ④	**R$ 7.243.702,96**	**R$ 5.028.751,68**	**R$ 5.777.984,80**	**R$ 3.424.852,05**	**R$ 2.620.000,00**
				Valor Total Estimado da Contratação:	**R$ 24.095.291.49**

① Quantidade estimada a partir do levantamento de demanda realizado junto aos Tribunais Participantes (Anexo B).
② Para o TRE/MA foram utilizados os valores estimados da contratação.
③ Média dos valores válidos considerados (vide critérios acima relacionados).
④ Calculado a partir da multiplicação de ① por ③.
⑤ Produto Oracle utilizado como referência.

ANEXO D – CONFIGURAÇÕES DO AMBIENTE DA CONTRATANTE

Oracle Database:	Enterprise Edition 18.12.2.0.0 e superior
Sistema Operacional:	A solução deverá ser homologada para o(s) seguinte(s) sistema(s) operacional(is): Oracle Linux Server 7.9 ou superior
Processador: ***(parâmetro referencial, baseado no ambiente dos TREs de tamanho médio)***	A solução deverá ser compatível com o(s) processador(es): product: Intel(R) Xeon(R) Gold 5222 CPU 3.80GHz (8 cores) vendor: Intel Corp.

ANEXO E – MEMÓRIA DE CÁLCULO

1. A definição de quantitativos de licenças para os produtos da presente contratação está atrelada à métrica de licenciamento adotada nos servidores que hospedam o Oracle Database.
2. Para fins de cálculo referencial, neste procedimento, adotam-se os seguintes critérios de licenciamento do Oracle Database:
    a. Métrica de licenciamento: Processador;
    b. Versão: *Oracle Database Enterprise Edition*;
    b. Hardware: 02 (dois) processadores com 04 (quatro) *"cores"* (núcleos) cada (parâmetro referencial, baseado no ambiente dos TREs de tamanho médio);
    b. Plataforma do hardware: Intel (parâmetro referencial, baseado no ambiente dos TREs de tamanho médio).
3. Para todos os produtos, a forma de cálculo na métrica "Processador" se dá do mesmo modo: somando-se os *"cores"* (núcleos) dos processadores do hardware. No caso do item 1, 2, e 3, o hardware é o servidor de banco de dados em que se utilizarão os produtos;
4. Para o item 4 – considerando-se, como referência, o produto *Oracle Audit Vault and Database Firewall* –, os servidores de banco de dados que serão protegidos. Salienta-se que, este estudo sugere que a contratação deste item seja "aberta", permitindo a participação de outros fabricantes. Neste caso, a métrica de licenciamento deste item específico poderá variar.
5. Em seguida multiplica-se este valor pelo fator de licenciamento de processador, existente na "Oracle Processor Core Factor Table". Busca-se a plataforma na tabela e o fator correspondente para o cálculo do número de licenças necessárias.
6. Deste modo, o cálculo referencial do total de licenças necessárias para cada produto seguem as regras a seguir:
7. Salienta-se que esta memória de cálculo de aplica tanto a determinar o quantitativo de licenças de servidores Oracle Enterprise Database quanto dos *packs* e *options* Oracle (itens 1 a 3). Deste modo, na prática, as quantidades de licenças de cada item de *pack* ou *option* corresponde ao número de licenças de Oracle Enterprise Database que cada Tribunal Participante deseja proteger.

Item	Descrição	Métrica	Hardware a considerar	Plataforma	Cálculo para o quantitativo de licenças	Alvo da Licença
1	Oracle Advanced Security	Processador	Servidor do Oracle Database	Intel	Nº Licenças = 2 processadores x 4 cores = 8 x 0,5 (plataforma) = 4	Host do Oracle Database
2	Oracle Data Masking and Subsetting Pack	Processador	Servidor do Oracle Database	Intel	Nº Licenças = 2 processadores x 4 cores = 8 x 0,5 (plataforma) = 4	Host do Oracle Database
3	Oracle Database Vault	Processador	Servidor do Oracle Database	Intel	Nº Licenças = 2 processadores x 4 cores = 8 x 0,5 (plataforma) = 4	Host do Oracle Database.
4	Oracle Audit Vault and Database Firewall	Processador	Servidores Protegidos	Intel	Nº Licenças = 2 processadores x 4 cores = 8 x 0,5 (plataforma) = 4	Host do Oracle Database

Fontes:

- https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dblic/Licensing-Information.html#GUID-68A4128C-4F52-4441-8BC0-A66F5B3EEC35
- https://www.oracle.com/cloud/price-list.html#data-safe
- https://www.oracle.com/a/ocom/docs/corporate/oracle-software-licensing-basics.pdf
- https://www.oracle.com/corporate/pricing/specialty-topics.html
- https://docs.oracle.com/en/database/oracle/oracle-database/19/dblic/Licensing-Information.html#GUID-B6113390-9586-46D7-9008-DCC9EDA45AB4

REFERÊNCIAS

[1] Resolução CNJ nº 182/2013. Disponível em: https://atos.cnj.jus.br/atos/detalhar/1874. Acesso nesta data.
[2] TCU, SEFTI. **Guia de Boas Práticas em Contratações de Soluções de Tecnologia da Informação**. 1. ed., Brasília, DF, 2012. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/guia-de-boas-praticas-em-contratacao-de-solucoes-de-tecnologia-da-informacao-1-edicao.htm. Acesso em: 18 de jul de 2022.
[3] Lei nº 13.709/2018 (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso nesta data.
[4] Decreto nº 9.637/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso nesta data.
[5] Resolução CNJ nº 363/2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso nesta data.
[6] Resolução TSE nº 23.650/2021. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-650-de-9-de-setembro-de-2021. Acesso nesta data.
[8] Resolução nº 23.644/2021. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021. Acesso nesta data.
[9] Instrução Normativa SGD-ME nº 1/2019. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019. Acesso em 10 de agosto de 2022.
[10] Vide: https://www.peerspot.com/. Acesso em 25/05/2022.
[11] Vide: https://www.peerspot.com/products/imperva-securesphere-database-security-reviews#review_119127. Acesso em 25/05/2022.
[12] Fonte: http://comprasnet.gov.br/ConsultaLicitacoes/ConsLicitacao_RelacaoTexto.asp. Acesso em 07/04/2022.
[13] GOVERNO DIGITAL. **Catálogo de Soluções de TIC**, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic#Oracle. Acesso em: 19 de jul de 2022.
[14] Acordo Corporativo nº 10/2021 entre a União e a Oracle do Brasil Sistemas Ltda. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/1-acordo-10-2021-com-dou.pdf Acesso em 25/05/2022.
[15] Catálogo de Soluções de TIC com condições padronizadas (ORACLE). Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-oracle-2021-v3.pdf. Acesso em 25/05/2022.
[16] Termo de Adesão ao Acordo nº 10/2021 - TRE/MG. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/termo-adesao-tre-mg-oracle.pdf Acesso em 19/07/2022.
[17] Fonte: https://partner-finder.oracle.com/catalog
[18] Fonte: https://www.oracle.com/a/ocom/docs/corporate/oracle-software-licensing-basics.pdf