ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA

1.1. DESCRIÇÃO SUCINTA

1.1.1. 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 no TRE-ES.

1.2. JUSTIFICATIVA DA NECESSIDADE

1.2.1. Necessidade 01: Aprimorar medidas técnicas de segurança da informação visando defesa, proteção e monitoramento de dados organizacionais nos bancos de dados Oracle hospedados no site da contratante e assegurar que estejam em conformidade com os normativos a seguir:

a) Lei nº 13.709/2018: Lei Geral de Proteção de Dados (LGPD);
b) Decreto nº 9.637/2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
c) 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;
d) Resolução TSE nº 23650/2021: Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;
e) Resolução nº 23.644/2021: Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

1.2.2. Necessidade 02: Assegurar à equipe de administradores de banco de dados Oracle o instrumental adequado para a condução de projetos em convergência com o macrodesafio: "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados do Planejamento Estratégico 2021-2026 (Tribunal Regional Eleitoral), Resolução TRE-ES Nº 94/2021", bem como operacionalizar diretrizes e recomendações da Política de Segurança a Informação.

1.3. RESULTADOS ESPERADOS

1.3.1. 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.

1.3.2. 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;

1.3.3. 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.

1.4. FUNDAMENTAÇÃO LEGAL

a) Lei nº 13.709/2018: Lei Geral de Proteção de Dados (LGPD);
b) Decreto nº 9.637/2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
c) 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;
d) Resolução TSE nº 23650/2021: Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;
e) Resolução nº 23.644/2021: Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

1.5. REFERÊNCIAS TÉCNICAS

a) NBR ISO/IEC 27001:2013;
b) NBR ISO/IEC 27002:2013;
c) NBR ISO/IEC 27005:2019

2. ESPECIFICAÇÃO DOS REQUISITOS

2.1. 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.

2.2. 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
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 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.
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.004;RL.010;RL.011

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.
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 Subconjuntos 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.

Id	Requisito
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.
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, registrarpa, alertará, substituirá ou bloqueiará a instrução.

Id	Requisito
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 rodar deve se conformar ao ambiente tecnológico e físico que está em operação na contratante.
RA.002	A solução deverá atuar na camada de banco de dados sem comprometer o desempenho dos bancos de dados da contratante.
RA.003	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 implicar na alteração de nenhuma das ferramentas já utilizadas para a administração de banco de dados Oracle utilizadas atualmente.
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 por um período de 12 meses, renovável até o limite de 12 meses.
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 por um período mínimo de 12 meses.
RT.002	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.

2.10. 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, 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.
RS.006	A contratada, na hipótese de ter que vir a atuar no contrato e ter que vir a ter contato com banco de dados da contratante, deverá assinar o termo de ciência e aceite do termo de compromisso de manutenção de sigilo e do código de ética da contratante.

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 C.
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 TI

3.1. ELEMENTOS DA STIC

3.1.1. 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 no TRE-ES;
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 SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO

4.1. ANÁLISE DE ADERÊNCIA AOS REQUISITOS FUNCIONAIS

4.1.1. Os requisitos funcionais da solução de tecnologia da informação a ser contratada aprimoram o segurança da informação foram agrupados nos nas 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).

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

Tabela 1. Análise de produtos de software

#	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	N
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	P
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. CONSIDERAÇÕES

4.2.1. A **Tabela 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.

4.2.2. A análise da tabela 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.

4.2.3. 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.ARQ003 que trata de arquitetura específica do *Oracle Database Enterprise Edition*;
b) As candidatas preferenciais serão aquelas que tiverem 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.

5. INDICAÇÃO DA STIC ESCOLHIDA

5.1. CARACTERIZAÇÃO DA SOLUÇÃO ESCOLHIDA

5.1.1. A solução escolhida é composta pelos produtos:

a) Oracle Advanced Security
b) Oracle Data Masking and Subsetting Pack
c) Database Vault
d) Oracle Audit Vault and Database Firewall

5.1.2. Informações adicionais:

a) Fornecedor: Existem dezenas de parceiros de revenda de licenças no Brasil (fonte: https://partner-finder.oracle.com/catalog), dos quais enumeram-se no ANEXO A aqueles que atendem o setor público.
b) Entidade proprietária da solução: Oracle
c) Estimativa de Orçamento: R$ XXX, conforme
d) Aderência da Solução ao MNI, ao ICP-Brasil e ao Moreq-Jus: Não se aplica.

5.2. JUSTIFICATIVAS DA ESCOLHA DA STIC

a) 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 deste tribunal: *Oracle Advanced Security*, *Oracle Data Masking and Subsetting Pack*, *Oracle Database Vault*. Estes programas são denominados 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,

b) 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. A característica determinante para escolha do *Oracle Audit Vault & Database Firewall* é a compatibilidade com a arquitetura tecnológica adotada pelo Tribunal e com demais itens da contratação, além de possibilitar o reconhecimento de comandos SQL em trânsito criptografados pela tecnologia Oracle Net.

5.2.1. 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.

5.3. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

5.3.1. 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.

5.3.2. 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 neste Tribunal Regional.

5.3.3. 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.

5.4. DESCRIÇÃO DA SOLUÇÃO

Item	Descrição
1	Oracle Advanced Security – Licença de perpétuo com suporte e atualização de software por 12 meses
2	Oracle Data Masking and Subsetting Pack – Licença de perpétuo com suporte e atualização de software por 12 meses
3	Oracle Database Vault – Licença de perpétuo com suporte e atualização de software por por 12 meses
4	Oracle Audit Vault and Database Firewall – Licença de perpétuo com suporte e atualização de software por 12 meses

5.5. RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

5.5.1. 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.

5.5.2. No Anexo C consta a memória de cálculo pela qual se chegou à seguinte demanda:

Item	Descrição	Métrica	Quantidade	Unidade de Medida
1	Oracle Advanced Security – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	Processador	04	Unidade
2	Oracle Data Masking and Subsetting Pack – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	Processador	04	Unidade
3	Oracle Database Vault – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	Processador	04	Unidade
4	Oracle Audit Vault and Database Firewall – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	Processador	04	Unidade

6. 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	Oracle Audit Vault and Database Firewall	Ambiente de Virtualização Requisitos de Memória: cada servidor x86 64-bit deve ter minimamente: a) Audit Vault Server: 8 GB b) Database Firewall: 8 GB Requisitos de Espaço: cada servidor x86 64-bit deve ter um único hard drive com o mínimo descrito a seguir: c) Audit Vault Server: 220 GB d) Database Firewall: 220 GB 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 E ESTRATÉGIAS DE MITIGAÇÃO

7.1. IDENTIFICAÇÃO E ANÁLISE DE RISCOS

RISCO 1	Uso inadequado/insuficiente da solução de TIC	
Probabilidade (Alta, média ou baixa)	Alta	
	Efeito (Dano)	*Impacto
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	Responsável Coordenadoria de Infraestrutura
2	Definir papéis e responsabilidades no uso da solução de TIC	Responsável Seção de Banco de Dados
3	Elaborar plano de implantação da solução de TI	Responsável Coordenadoria de Infraestrutura Responsável Seção de Banco de Dados

*Impacto (Baixo, Médio ou Alto)

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
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	Responsável Coordenadoria de Infraestrutura
2	Definir rotina para atualização de solução durante vigência contratual	Responsável Seção de Banco de Dados
3	Acompanhar vigência contratual	Gestor do Contrato

*Impacto (Baixo, Médio ou Alto)

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
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	Responsável Coordenadoria de Infraestrutura
2	Definir rotina para atualização de solução durante vigência contratual	Responsável Seção de Banco de Dados
3	Acompanhar vigência contratual	Gestor do Contrato

*Impacto (Baixo, Médio ou Alto)

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
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”	Responsável Coordenadoria de Infraestrutura
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

*Impacto (Baixo, Médio ou Alto)

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
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.	Responsável Coordenadoria de Infraestrutura
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 Responsável Coordenadoria de Infraestrutura

*Impacto (Baixo, Médio ou Alto)

7.2. DESCONTINUIDADE DO FORNECIMENTO

7.2.1. 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.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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

8.1. DA RENOVAÇÃO DE LICENÇAS DA STIC

8.1.1. 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.

8.1.2. O reestabelecimento do acesso aos serviços citados demandará por novo processo licitatório, conduzido anualmente, cujo custo estimado é de aproximadamente 22% (vinte de dois por cento) do custo da presente contratação. Fonte: https://www.oracle.com/a/ocom/docs/corporate/oracle-software-licensing-basics.pdf

8.2. DAS MEDIDAS DE PRESERVAÇÃO DE INVESTIMENTO

8.2.1. 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 da equipe de Banco de Dados e da equipe de Segurança.

9. RECURSOS MATERIAIS E HUMANOS

9.1. RECURSOS MATERIAIS

9.1.1. Adicionalmente aos recursos materiais descritos em INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL, devem ser considerados:

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

9.2. RECURSOS HUMANOS

9.2.1. Alocação de equipe capacitada e dedicada à implantação e uso da solução de TIC;

9.2.2. Alocação de equipe capacitada e dedicada ao uso da solução de TIC;

9.2.3. Alocação de gerente de projetos para a implantação da solução de TIC.

A. LISTA DE PONTENCIAIS FORNECEDORES

Fornecedor	Contato
Accenture do Brasil Ltda.	patricia.costa.nunes@accenture.com
Accerte Tecnologia Da Informacao Ltda-epp	licitacoes@accerte.com.br
Advanced Database & IT Sistemas De Informacao S A	comercial@advancedit.com.br
Ax4b Sistemas De Informatica Ltda	Romulo.oliveira@ax4b.com
Bb Tecnologia E Servicos S.A	comercial@bbts.com.br
Bertini Do Brasil Ltda	nereu.monteiro@bertini.com.br
Centurylink Comunicações do Brasil Ltda	contato.br@lumen.com
Compethics It Solucoes Em Tecnologia Da Informacao Eireli	alexandre_piano@lta-rh.com.br
Compwire Informatica S/A	contato@compwire.com.br
CSI CENTRO DE SOLUCOES EM INFORMATICA LTDA	almir.carone@csiway.com.br
CSI Inovacao Em Ti Eireli	almir.carone@csiway.com.br
First Decision Tecnologias Inovadoras E Informatica Ltda	juliano.korff@firstdecision.com.br
G&P Projetos E Sistemas S.A.	comercial@gpnet.com.br
Halbar Solucoes Em Tecnologia Da Informacao Eireli	alexandre_piano@lta-rh.com.br
IT-One Tecnologia Da Informacao S.A.	edgar.luiz@itone.com.br
Ka Solution Informática Ltda	
Lanlink Solucoes E Comercializacao Em Informatica S/A	kleper.Porto@lanlink.com.br
LTA-RH INFORMATICA, COMERCIO, REPRESENTACOES LTDA	alexandre_piano@lta-rh.com.br
Magna Sistemas Consultoria S/A	rghashimoto@magnasistemas.com.br
NEC Latin America S.A.	
Netmanagement Informatica Ltda - Epp	licitacoes@datacentrics.com.br
Philips Clinical Informatics - Sistemas De Informacao Ltda	Leila.Duflot@philips.com
Service Informatica Ltda.	contato@service.com.br
SQL Intelligence Consultoria Ltda	robinson.simoes@sqltech.com.br
Sumauma Computadores E Telecomunicacoes Ltda	tatiana@sumaumatelecom.com.br
Tecnocomp Tecnologia E Servicos Ltda	mauro.marsura@tecnocomp.com.br
TIVIT Terceirizacao de Processos, Servicos e Tecnologia SA	comercialsalesbrazil@tivit.com
TLD Teledata Tecnologia em Conectividade Eireli	comercial.gov@teledatabrasl.com.br

To Brasil Consultoria Em Tecnologia Da Informacao Ltda	cristina.paderni@to-brasil.com
V2 Tecnologia Ltda	comercial@v2com.com
V8 Consulting Ltda	comercial@v8consulting.com.br
VS DATA COMERCIO & DISTRIBUICAO LTDA	governo@vsdata.com.br
Wipro Do Brasil Sistemas De Informatica LTDA	rodrigo.reis2@wipro.com
Wipro Do Brasil Tecnologia Ltda	rodrigo.reis2@wipro.com

B. CONTRATAÇÕES PÚBLICAS SIMILARES

#	Órgão	Pregão em	Pregão	Localizador
1	Tribunal Regional Eleitoral do Maranhão	Set/2021	Pregão: 30/2021 UASG: 70005	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=70005&modprp=5&numprp=302021
2	Empresa de Tecnologia da Informação do Ceará ETICE	Ago/2021	Pregão: 415/2021 UASG: 943001	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=943001&modprp=5&numprp=41520 21
3	Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis	Out/2018	Pregão: 23/2018 UASG: 193099	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=193099&modprp=5&numprp=23201 8
4	Governo do Estado do Ceará	Dez/2017	Pregão: 1365/2017 UASG: 943001	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=943001&modprp=5&numprp=13652 017
	Fundo de Imprensa Nacional	Fev/2017	Pregão: 1/2017 UASG: 110245	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=110245&modprp=5&numprp=12017

Consulta em: http://comprasnet.gov.br/ConsultaLicitacoes/ConsLicitacao_RelacaoTexto.asp, em 07/04/2022.
Chave de Busca: “Oracle Security”

C. ESTIMATIVA DE PREÇOS

Item	Produto de Software	Métrica	Preço Unitário[1] (R$)	Quantitativo de Licenças	Valor (R$)
1	Oracle Advanced Security	Por processador	R$ 65.943,44	4	R$ 263.773,76
2	Data Masking	Por processador	R$ 50.556,64	4	R$ 202.226,56
3	Database Vault	Por processador	R$ 50.556,64	4	R$ 202.226,56
4	Audit Vault and Database Firewall	Por processador	R$ 26.377,38	4	R$ 105.509,52
Estimativa do Total da Contratação					R$ 773.736,40

(1) Com base na Ata de Registro de Preço decorrente do Pregão 415/2021

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	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.

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. Nesta regional, os servidores que hospedam o Oracle Database adotam o seguinte licenciamento:
   2.1. Métrica de licenciamento: Processador;
   2.2. Versão: *Oracle Database Enterprise Edition*;
   2.3. Hardware: 02 (dois) processadores com 04 (quatro) *"cores"* (núcleos) cada;
   2.4. Plataforma do Hardware: Intel.
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; para o item 4, os servidores de banco de dados que serão protegidos. Em seguida multiplica-se este valor pelo fator de licenciamento de processador, existente na "Oracle Processor Core Factor Table" (Anexo C). Busca-se a plataforma na tabela e o fator correspondente para o cálculo do número de licenças necessárias.
4. O cálculo do total de licenças necessárias para cada produto seguem as regras a seguir:

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		
2	Oracle Data Masking and Subsetting Pack	Processador	Servidor do Oracle Database	Intel		Oracle Database
3	Oracle Audit Vault and Database Firewall	Processador	Servidores Protegidos	Intel		Host do Oracle Database
4	Oracle Database Vault	Processador	Servidor do Oracle Database	Intel		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

Oracle Advanced Security – Licença de perpétuo com suporte e atualização de software por 01 (um) ano
Oracle Data Masking and Subsetting Pack – Licença de perpétuo com suporte e atualização de software por 01 (um) ano
Oracle Audit Vault and Database Firewall – Licença de perpétuo com suporte e atualização de software por 01 (um) ano
Oracle Database Vault – Licença de perpétuo com suporte e atualização de software por 01 (um) ano

9.2.4. Segundo o documento “Database Licensing” (Anexo XXX), o Oracle Database Enterprise Edition possui duas métricas possíveis para licenciamento: “Named User Plus” ou “Processor”. A métrica utilizada para licenciar os produtos “Named User Plus” é preciso identificar e contar os usuários que terão acesso ao banco de dados para que seja possível calcular a quantidade de licenças necessárias para a legalização do SGBD. Com o uso da internet, é impossível fazer essa identificação e contagem. Como o servidor secundário pode assumir o papel do servidor primário, e, portanto, provê acesso a dados pela internet, a métrica utilizada para o licenciamento do servidor secundário é a métrica “Processor”, mesma do servidor primário.

O cálculo do número de licenças necessárias utilizando a métrica “Processor” é feito da seguinte forma: multiplica-se o número total de cores do servidor de banco de dados pelo fator de licenciamento de processador, existente na “Oracle Processor Core Factor Table” (Anexo C). O tipo da máquina servidora deve ser identificado na tabela e o fator relacionado a ela deve ser usado no cálculo do número de licenças necessárias.

O servidor de banco de dados secundário possui a seguinte configuração: Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (6 Cores). Assim, pela tabela, o fator utilizado é 0,5. Como a máquina possui 6 cores, o cálculo fica da seguinte maneira:

Nº Licenças = 6 (nº de cores) x 0,5 (fator) = 3

Item	Descrição	Cálculo
1	Oracle Advanced Security – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	Total de processadores: 2 Total de núcleos por servidor
2	Oracle Data Masking and Subsetting Pack – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	
3	Oracle Audit Vault and Database Firewall – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	
4	Oracle Database Vault – Licença de perpétuo com suporte e atualização de software por 01 (um) ano	

F. PRODUTOS DE SEGURANÇA ORACLE

Feature / Option / Pack	EE	Notes
Transparent Data Encryption (TDE) for Columns	Y	EE and EE-Exa: Requires the Oracle Advanced Security option
Transparent Data Encryption (TDE) for Tablespaces	Y	EE and EE-Exa: Requires the Oracle Advanced Security option
Oracle Advanced Security	Y	EE and EE-Exa: Extra cost option
Oracle Database Vault	Y	EE and EE-Exa: Extra cost option
Oracle Label Security	Y	EE and EE-Exa: Extra cost option
Redaction	Y	EE and EE-Exa: Requires the Oracle Advanced Security option

Fonte: Adaptado de: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dblic/Licensing-Information.html#GUID-0F9EB85D-4610-4EDF-89C2-4916A0E7AC87

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria DG nº <número, referência SEI>)

Integrante Demandante: <Nome do titular> (substituto: <Nome do substituto>)

Integrante Técnico: <Nome do titular> (substituto: <Nome do substituto>)

Integrante Administrativo: <Nome do titular> (substituto: <Nome do substituto>)