



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA (DOD)

1. Objeto: Contratação de itens de segurança para SGBD ORACLE

Descrição sumária: Contratação de módulos adicionais de segurança para bancos de dados ORACLE.

Unidade Demandante: SEÇÃO DE ADMINISTRAÇÃO DE DADOS E INTELIGÊNCIA DE NEGÓCIO - SADIN

Servidor responsável pela oficialização da demanda: Luciano Barros Queiroz

2. A demanda foi prevista no Plano Anual de Contratação?

A referida demanda não foi incluída no PAC, pois foi uma diretriz colocada pelo TSE há pouco tempo e cuja contratação está sendo encabeçada pelo TRE-CE.

3. Motivação da contratação e demonstrativo dos resultados que serão alcançados (considerando o Planejamento Estratégico)

Motivação: O sistema de gerenciamento de banco de dados (SGBD) Oracle que está presente em todos os regionais da JE, bem como no TSE, atualmente encontra-se sem a contratação dos módulos de segurança específicos do mesmo, contando apenas com a proteção provida por outros sistemas gerais de segurança.

Busca-se, por meio da contratação, conformidade com os normativos elencados a seguir, tratando da questão da segurança e da proteção da privacidade dos dados sob custódia dos TREs, no escopo de dados armazenados em bancos de dados Oracle:

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

Na motivação de conformidade aos normativos referenciados, a problemática da salvaguarda de direito à privacidade dos cidadãos e da reputação institucional subsidiada pela proteção dos ativos de informação. A proteção passa pela necessidade-dever de prover mecanismos adequados de segurança para as instâncias de armazenamento para onde fluem os dados coletados e tratados nas mais diversas soluções corporativas hospedadas na infraestrutura dos tribunais eleitorais; em suma, segurança para os bancos



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

de dados.

O objeto desta contratação é composto por programas conhecidos como “*options*”, que permitem o uso de recursos adicionais de segurança para os dados armazenados no “Oracle Database”. O Oracle Database é um sistema de gerenciamento de banco de dados ao qual parte significativa das soluções da Justiça Eleitoral, cujas seminais datam de meados da década de 1990, é estruturalmente acoplada, gerando estreita dependência tecnológica das soluções ao produto. A adoção do Oracle Database tornou-se mandatória – como um padrão “de facto” – para os Tribunais Regionais Eleitorais, uma vez que devem consumir soluções providas, de modo compulsório e uniformizado, pelo Tribunal Superior Eleitoral e, de outro lado, necessitam prover soluções internas complementares às do TSE e, ainda, venham a ter pretensão de compartilhar estas soluções complementares com seus pares eleitorais. Consequentemente, o produto Oracle Database é mantido e utilizado neste e nos demais TREs participantes desta contratação.

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

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

A contratação proposta, por meio da aquisição de licenças para produtos que permitem o aprimoramento da proteção de dados, do controle de acesso aos dados, da auditoria e do monitoramento dos ativos de informação, pilares da segurança e privacidade, visa a obter os resultados descritos no quadro a seguir relativos à segurança dos bancos de dados Oracle.



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

Resultados que serão alcançados:

PILAR DE CIBERSEGURANÇA:	Proteção de Dados
Requisitos do Programa	Resultados esperados
<ul style="list-style-type: none">● Criptografia dos arquivos de armazenamento de dados;● Criptografia na geração de arquivos de backups;● Criptografia na geração de arquivos de exportação. <ul style="list-style-type: none">● Tratamento dos dados, por meio de mascaramento ou reescrita antes da entrega do dado ao solicitante.● Mascaramento irreversível de dados;● Empacotamento de um subconjunto consistente de dados a partir da totalidade de dados existentes. <ul style="list-style-type: none">● Segregação de papéis no banco de	<ul style="list-style-type: none">● Proteção contra exposição de dados decorrentes de roubo, perda, sequestro de mídia de armazenamento e backups de banco de dados roubados ou perdidos;● Proteção contra exposição de dados roubados diretamente pelo sistema operacional;● Proteção contra leituras indevidas diretamente pelo sistema operacional por meio de contas privilegiadas de sistema operacional;● Proteção na entrega de dados a terceiros, garantindo o acesso somente a quem de direito;● Proteção contra leituras indevidas de backups armazenados. <ul style="list-style-type: none">● Restrição de acesso a dados sensíveis diretamente na requisição de dados, sem que haja necessidade de revisão (manutenção) de sistemas corporativos que o acessam;● Restrição de acesso a dados sensíveis às consultas executadas por ferramentas de acesso direto ao banco de dados;● Proteção contra exposição de dados acessados ou roubados de ambiente não produtivos (homologação e desenvolvimento);● Proteção contra uso indevido de informações privilegiadas de infraestrutura de banco de dados. Por exemplo: volumetria, densidade, histograma;● Proteção de dados, por meio de anonimização, quando enviados para terceiros ou a desenvolvedores;● Contenção dos dados críticos ao ambiente produtivo, reduzindo pontos de roubo de dados. <ul style="list-style-type: none">● Proteção dos dados contra leituras indevidas por contas



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

<p>dados;</p> <ul style="list-style-type: none">● Controle de privilégios de administração;● Delimitação de “territórios” de acesso aos dados;● Classificação dos dados de acordo com categorias definidas em nível de registro de BD. <ul style="list-style-type: none">● Auditoria unificada de acessos aos dados do banco de dados;● Política de segurança dos dados a partir de definição de perímetro de rede, usuários, aplicações● Política de segurança baseado em comandos de busca	<ul style="list-style-type: none">de administração no banco de dados;● Proteção contra erros ocasionados por excesso de privilégios;● Proteção contra-ataques e roubos originados de pessoas que atuam dentro órgão;● Redução de danos em caso de extravio ou divulgação de contas de administração;● Contenção de atuação de contas de administração”;● Definição de “territórios” para contas de aplicação, reduzindo necessidade de concessão de privilégios diretos;● Controle de acesso ao banco de dados em nível de registro de acordo com a classificação atribuída e o perfil do usuário. <ul style="list-style-type: none">● Prevenção ativa de acessos indevidos;● Restrição prévia de acessos indevidos, baseada em política de segurança que envolva restrições de acesso de horário, IPs, aplicações, contas;● Coleta unificada de auditoria de dados sensíveis, com histórico de acesso;● Prevenção ativa de execução de comandos em linguagem SQL a partir de contas autorizadas.
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4. Objetivo estratégico a ser atendido

OE 3 - Fortalecimento da segurança do processo eleitoral

Além do atendimento às normas elencadas na motivação da contratação

5. Grau de prioridade da demanda

Essencial

5.1. Prazos estimados:

Data prevista para ETP definitivo: Por se tratar de contratação em que constamos como partícipes, o ETP já consta neste processo.

Data prevista para TR definitivo: Por se tratar de contratação em que constamos como partícipes, o TR já consta neste processo.

Data prevista para contratação/aquisição: 30 de novembro de 2022.



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

6. Vinculação com outra contratação?

Esta contratação será efetuada através de um Registro de Preços e está sendo liderada pelo TRE-CE, onde o TRE-PR está como partícipe no processo.

7. Equipe de Planejamento da Contratação

Área Demandante: SADIN

Servidor Demandante/Líder do Planejamento: Luciano Barros Queiroz

Integrante Técnico: Marcelo da Silva Volaco

Integrante Administrativo: a ser indicado pela SECAD

8. Detalhamento do Objeto

Descrição do objeto: Aquisição de licenças *Oracle Advanced Security*; *Oracle Data Masking and Subsetting Pack* e *Oracle Database Vault*.

Quantidade estimada:

- **Oracle Advanced Security:** 4
- **Oracle Data Masking and Subsetting Pack:** 4
- **Oracle Database Vault:** 4

Local de entrega ou da prestação dos serviços: Sede TRE-PR

9. Informação preliminar de preço

Conforme cotação preliminar constante no TR da contratação liderada pelo TRE-CE, os valores unitários da contratação são:

- **Oracle Advanced Security:** R\$ 69.650,99
- **Oracle Data Masking and Subsetting Pack:** R\$ 52.382,83
- **Oracle Database Vault:** R\$ 51.589,15

Totalizando: R\$ 694.491,88 (173.622,97 por licença)

Curitiba, 24 de agosto de 2022.



Tribunal Regional Eleitoral do Paraná

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

Chefe da Seção demandante: LUCIANO BARROS QUEIROZ

Coordenador demandante: DESIREE HERNANDEZ MAUSBACH RICCO

Secretário demandante: GILMAR JOSE FERNANDES DE DEUS