TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO

DOD – Documento de Oficialização de Demanda

PREENCHIMENTO PELA ÁREA REQUISITANTE

1 – IDENTIFICAÇÃO DA ÁREA REQUISITANTE

Área Requisitante (Unidade/Setor/Departamento): **Coordenadoria de Sistemas e Inovação - COSIN**

Responsável pela demanda: **Egídio de Carvalho Ribeiro Júnior**

Matrícula: **30990088**

E-mail: ***egidio.carvalho@tre-ma.jus.br***

Telefone: **(98) 2107 8957** Data da elaboração do documento: **30/05/2022**

2 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE

Nome: **Egídio de Carvalho Ribeiro Júnior** Matrícula: **30990088**

Cargo: **Coordenador de Sistemas e Inovação** Lotação: **COSIN**

E-mail: ***egidio.carvalho@tre-ma.jus.br***

Telefone: **(98) 2107 8957**

Por este instrumento, declaro ter ciência das competências do INTEGRANTE REQUISITANTE, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

_____

Egídio de Carvalho Ribeiro Júnior
Integrante Requisitante

3 – IDENTIFICAÇÃO DA DEMANDA

Necessidade de contratação de atualização e suporte do software por 48 meses das seguintes options de segurança:

I – Oracle Advanced Security - Processor Perpetual

II – Oracle Data Masking and Subsetting Pack - Processor Perpetual

III – Oracle Audit Vault and Database Firewall - Processor Perpetual

ALINHAMENTO ESTRATÉGICO DA CONTRATAÇÃO

Alinhamento Estratégico Institucional

A necessidade da presente contratação encontra-se alinhada com os seguintes normativos e instrumentos estratégicos:

- Normativos correlatos à segurança de dados na internet, especialmente
  - **Resolução CNJ nº 290/2021**, que trata do protocolo de gerenciamento de crises cibernéticas no âmbito do Poder Judiciário.
  - **Resolução CNJ nº 291/2021**, que trata do protocolo de investigação de ilícitos cibernéticos no âmbito do Poder Judiciário
  - **Resolução CNJ nº 292/2021**, CNJ que trata do protocolo de prevenção de incidentes cibernéticos no âmbito do Poder Judiciário.
  - **Resolução CNJ nº 325/2020, de 29/06/2020,** que trata da estratégia Nacional do Poder Judiciário 2021-2026
  - **Resolução CNJ nº 370/2021 (ENTIC-JUD),** que trata da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD), conforme objetivos indicados adiante:
    - Perspectiva: **Processos internos** – Objetivo: **2-Aprimorar a segurança da informação e a gestão de dados**
  - **Resolução CNJ nº 396/2021 (ENSEC-PJ)**, que trata da estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)
  - **LGPD – Lei Geral de Proteção de Dados,** que é a lei brasileira que regulamenta questões relacionadas ao compartilhamento, tratamento e armazenamento de dados
  - **Programa Nacional de Cibersegurança da Justiça Eleitoral – TSE**, baseada em cinco eixos estruturantes, a saber: (1) pessoas e unidades organizacionais, (2) políticas e normatização, (3) ferramentas automatizadas, (4) serviços especializados, e (5) sensibilização e conscientização.
- Atender aos seguintes objetivos estratégicos do TRE-MA
  - **Plano Estratégico 2021-2026 do TRE-MA**
    - Perspectiva: **Gestão e Inovação** – Objetivo: **Aprimorar a Infraestrutura e Governança de TIC**
    - Perspectiva: **Gestão e Inovação** – Objetivo: **Promover a Proteção de Dados e Segurança Cibernétic**a
  - **PDTIC 2021-2026 do TRE-MA**
    - Definir e executar atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem
  - Demanda prevista no Plano de Contratações de TIC 2022, Lei Nº 14.303/2022

4 – MOTIVAÇÃO/JUSTIFICATIVA DA CONTRATAÇÃO

Busca-se, por meio da contratação, manter atualizadas as licenças de Options de segurança Oracle adquiridas por este TRE, mantendo conformidade com os normativos elencados a seguir, tratando da questão da segurança e da proteção da privacidade dos dados sob custódia do TRE-MA, no escopo de dados armazenados em bancos de dados Oracle:

a) Lei nº 13.709/2018: Lei Geral de Proteção de Dados (LGPD)9;

b) Resolução CNJ nº 363/202110: Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;

c) Resolução TSE nº 23650/202111: Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;

d) Resolução nº 23.644/202112: 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 de dados.

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

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, vez que devem consumir soluções providas, de modo compulsório e uniformizado, pelo Tribunal Superior Eleitoral e, de outro lado, necessitam prover soluções internas complementares às do TSE e, ainda, venham a ter pretensão de compartilhar estas soluções complementares com seus pares eleitorais. Consequentemente, o produto Oracle Database é mantido e utilizado neste TRE.

O Oracle Database fornece recursos elementares de segurança e auditoria para os seus bancos de dados. Entretanto, confrontado por um cenário de crescente ameaça aos ativos de informação, seja por ataques cibernéticos externos, seja por roubo ou extravio por pessoas acreditadas pela organização, e considerando os danos à imagem institucional e de

responsabilização do órgãos em caso de extravio, roubo, divulgação ou sequestro destes ativos, estabeleceu-se outro patamar, mais elevado, de requisitos para aprimoramento dos mecanismos de segurança, resultando na necessidade de extensão dos recursos de proteção do Oracle Database.

A extensão dos recursos de proteção do produto Oracle Database se dá pela oferta de programas nativos e integrados com recursos sofisticados de segurança e privacidade dos ativos de informação, alguns dos quais disponibilizados automaticamente no momento de sua própria instalação. Entretanto, para que se faça uso dos recursos avançados de segurança e privacidade providos por estes programas ao produto Oracle Database, torna-se imperativo o licenciamento prévio, de caráter individualizado, do contrário, o utilizador dos programas incorrerá em ilegalidade decorrente de infrações contratuais sujeitas a penalidades. Essa aquisição de licença de uso perpétuo dos referidos programas (*options*) foi feita por este Regional em novembro de 2001 (SEI Nº 0006458-98.2021.6.27.8000).

Esses programas(*options*) adquiridos permitem o aprimoramento da proteção de dados, do controle de acesso aos dados, da auditoria e do monitoramento dos ativos de informação, pilares da segurança e privacidade, visa a obter os resultados descritos a seguir na segurança dos bancos de dados Oracle (Quadro 1).

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

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

5 – RESULTADOS PRETENDIDOS

Quadro 1: Resultados esperados da contratação

PILAR DE CIBERSEGURANÇA: Proteção de Dados	
Recursos de segurança do programa	Resultados esperados
▪ Criptografia dos arquivos de armazenamento de dados; ▪ Criptografia na geração de arquivos de backups; ▪ Criptografia na geração de arquivos de exportação	▪ 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
▪ Tratamento dos dados, por meio de mascaramento ou reescrita antes da entrega do dado ao solicitante	▪ Restrição de acesso a dados sensíveis direta mente 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;
▪ Mascaramento irreversível de dados; ▪ Empacotamento de um subconjunto consistente de dados a partir da totalidade de dados existentes	▪ 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 da dos. 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
PILAR DE CIBERSEGURANÇA: Controle de acesso aos dados	
Recursos de segurança do programa	Resultados esperados
▪ Segregação de papéis no banco de dados; ▪ 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	▪ Proteção dos dados contra leituras indevidas por contas 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.

PILAR DE CIBERSEGURANÇA: Auditoria e Monitoramento	
Recursos de segurança do programa	Resultados esperados
▪ 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	▪ 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

Além dos benefícios acima citados, a presente contratação também ajudará no cumprimento das seguintes metas constantes no plano de diretrizes 2021-2022:

a) Índice de disponibilidade de serviços essenciais de TIC (98,99% em 2021 a 2026)
b) Disponibilidade do Serviço de Banco de Dados
c) Índice de Adesão à LGPD (25% em 2021; 50% em 2022; 75% em 2023; 100% em 2024)

6 – FONTE DE RECURSOS

Plano interno: INV SOFTWR - AQUISICAO E DESENVOLVIMENTO DE SOFTWARE. Natureza da despesa: 449040 - SERVICOS DE TECNOLOGIA DA INFORMACAO E COMUNICACAO – PJ

ENCAMINHAMENTO

Encaminhe-se ao Secretário de Tecnologia da Informação e Comunicação para providências.

Egídio de Carvalho Ribeiro Júnior

Titular da Área Requisitante da Demanda

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

7 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome**: Glaycy Anne de Melo Correia Costa**

Matrícula: **3099919** E-mail: ***glaycy.melo@tre-ma.jus.br*** Telefone: **(98) 2107-8877**

Cargo: **Técnico Judiciário** Lotação: **SEDIN**

Por este instrumento, declaro ter ciência das competências do INTEGRANTE TÉCNICO, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

_____

Glaycy Anne de Melo Correia Costa

Integrante Técnico

ENCAMINHAMENTO

Encaminhe-se à autoridade competente da Área Administrativa, que deverá:

I – Decidir motivadamente sobre o prosseguimento da contratação;

II – Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e

III – Instituir a Equipe de Planejamento da Contratação, na forma da legislação em vigor.

_____

Gualter Gonçalves Lopes Júnior

Secretário de Tecnologia da Informação e Comunicação