TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 20/2022 - TRE-ES/PRE/DG/STI/CSGIT/SAGGI

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

[Obrigatório mesmo para prorrogações, art. 19, § único, resolução TRE-ES nº 261/2018]

1. CARACTERIZAÇÃO DA DEMANDA

1.1. DESCRIÇÃO SUCINTA

1. Aquisição de uma Solução Integrada de Software para Gerenciamento de Processos de LGPD e Gerenciamento de Riscos e Conformidade (GRC).

1.2. DETALHAMENTO

Grupo	Item	Descrição	Qtde (Unidade)
1	1	Solução de Software para Gestão de LGPD e Gestão de Riscos e Conformidade (GRC), por ano de uso	1
	2	Consultoria para parametrização do sistema e implantação	1
	3	Workshop remoto	1

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

1. A Justiça Eleitoral é constantemente demandada por órgãos de controle, como CNJ e TCU, para aperfeiçoar os seus processos de gestão, sejam relacionados à governança corporativa, governança de TI, de segurança da informação e, mais recentemente, implementação de controles para privacidade, em atendimento à LGPD. Neste sentido, a gestão de riscos e de processos de tratamento de dados pessoais, feita atualmente de forma *ad-hoc*, manual e sem integração entre as áreas, é fonte de preocupação para os gestores. A demanda de gestão de riscos nas contratações coincidiu com a demanda na implementação de controles para LGPD, com a implementação mais aprimorada e um plano de continuidade de negócios e com controles de segurança da informação, ações estas constantes do PDTIC 2021-2026 do TRE/ES.

2. É mais adequado tratar estes processos de forma integrada, o que diminui o nível de retrabalho e aumenta a visibilidade dos riscos para a alta gestão. Devido a isto, foi realizada uma análise de soluções de mercado que contemplem todos estes públicos e que melhorem, num médio prazo, o resultado geral de governança corporativa no Tribunal. A solução será utilizada na melhoria dos processos de gestão de riscos corporativos, incluindo privacidade, segurança da informação, continuidade de negócios, aquisições, contratos, controles de indicadores estratégicos, ESG (Environmental, Social and Governance), entre outros, podendo ser utilizado pela alta gestão no monitoramento mais efetivo e no acompanhamento dos resultados.

3. A solução será utilizada na implementação dos controles de processos que atuam com dados pessoais, em conformidade com a LGPD, como mapeamento, gestão de incidentes, análise de riscos, controle de ativos e emissão automatizada de relatório de impacto de dados pessoais. A contratação por Registro de Preços foi escolhida para permitir a participação de outras entidades da administração pública federal.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1. REQUISITOS DE SEGURANÇA

1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644/2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Espírito Santo (TRE/ES) aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;
2. O TRE/ES terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;
3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX);

4. O fornecedor assinará um Termo de Confidencialidade em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei;
5. Todos os dados inseridos na aplicação serão de propriedade do TRE/ES, o fornecedor deverá fornecer estrutura adequada de distribuição de permissão de acesso e segurança das informações de forma que somente pessoas autorizadas tenham acesso, que na ocorrência de eventuais falhas ou desastres, as informações possam ser recuperadas em prazo razoável.

2.2. REQUISITOS GERAIS

1. O solicitado é uma **Solução Software para Gerenciamento de Processos de LGPD e Gerenciamento de Riscos e Conformidade (GRC),** disponibilizada como serviço em nuvem pública (SaaS - Software As A Service, Software como Serviço);
2. A proposta deverá contemplar todas as licenças para o uso do software, o suporte técnico, as atualizações tecnológicas do produto, a infraestrutura de nuvem utilizada, o treinamento e o serviço de configuração inicial;
3. A solução de software deve ser de mercado, pronta e operacional, não sendo admitido soluções criadas especificamente para esta contratação;
4. A CONTRATADA deverá estar autorizada pelo fabricante para comercializar e suportar a solução;
5. Qualquer terceirização dos serviços a serem prestados pela CONTRATADA deverá ser previamente acordado com os fiscais da CONTRATANTE, devendo os colaboradores envolvidos assinarem um Termo de Sigilo e Responsabilidade a ser emitido pela CONTRATANTE;
6. O tipo de licenciamento é **SaaS (Software as a Service),** devendo a CONTRATADA oferecer hospedagem em nuvem pública localizada em território nacional;
7. Deverá ser ofertada a última versão estável de todos os softwares;
8. Os técnicos alocados pela CONTRATADA para a realização de serviços deverão estar devidamente capacitados pelo fabricante da solução;
9. A solução deve estar disponível para uso em, no máximo, 10 dias após a assinatura do contrato;
10. A solução de software deve ser capaz de fazer a gestão de processos de LGPD e proteção de dados pessoais, de acordo com os requisitos técnicos constantes neste edital;
11. A solução de software deve ser capaz de fazer a gestão de riscos e conformidade, de acordo com os requisitos técnicos constantes neste edital;
12. O módulo de LGPD deve ser 100 % integrado ao módulo de GRC;
13. O tipo de licenciamento é contratação de **Software as a Service (SaaS),** com licenciamento anual, podendo ser contratado por um, dois ou três anos, de acordo com a quantidade adquirida;
14. Caso a solução leve em conta o número de funcionários do CONTRATANTE para o nível de licenciamento, deve considerar 700;
15. Deverá permitir a atualização para novas versões, consertos de falhas operacionais, conserto de vulnerabilidades de segurança e suporte técnico especializado;
16. A proposta deve incluir a configuração inicial, como criação de modelos de riscos, modelos de avaliação para processos de tratamento de dados pessoais, mapas de calor, formulários, configuração da autenticação de usuários, incluindo seus grupos e perfis;
17. A proposta deve incluir treinamentos para uso e administração da solução.

2.3. REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

1. A CONTRATADA deverá apresentar plano de treinamento para todos os usuários da solução, englobando LGPD, GRC e administração.

2.4. REQUISITOS DE MANUTENÇÃO E GARANTIA

1. O suporte para eventuais desconformidades, inoperância do software, indisponibilidade da ferramenta, correção das permissões de acesso e atualização das versões devem ser previstas em nível de serviço a serem definidos.

2.5. REQUISITOS TEMPORAIS

1. A solução deve estar disponível para uso em, no máximo, 10 dias após a assinatura do contrato;
2. A CONTRATADA deve efetuar as configurações mínimas em até 30 dias após a disponibilização da solução, ou conforme acordado com o gestor do contrato e definido no plano de implantação;
3. A contratação terá uma vigência de 12 meses com possibilidade de prorrogação.

2.6. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1. Não haverá compartilhamento de dados pessoais controlados pelo Tribunal com a futura contratada;
2. Não haverá acesso de informação sensíveis do Tribunal pela contratada;
3. Deverá ser incluído:
    1. MODELO do Termo de Compromisso de Manutenção de Sigilo a ser assinado pela empresa; e
    2. MODELO do Termo de Ciência e Aceite do Termo de compromisso de manutenção de sigilo e do código de ética do TRE/ES, a ser assinado por todos os profissionais da contratada que atuarem no contrato.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1. CARACTERÍSTICAS GERAIS

1. Softwares, infraestrutura de nuvem pública e suporte deverão ser fornecidos pela CONTRATADA;
2. Deve ser 100% baseado em plataforma Web compatível com o padrão W3C;
3. Deve suportar o idioma português brasileiro nas interfaces web, dashboards e relatórios;
4. Deve permitir acesso pelos navegadores Chrome, Firefox, Edge e Opera, em suas versões mais recentes, sem a necessidade de uso de plugins ou softwares adicionais instalados nos dispositivos clientes;
5. Deve utilizar o protocolo HTTPS, com suporte a TLS 1.2 ou superior;
6. Permitir a integração para autenticação de usuários com Active Directory, da Microsoft, versão 2016 Server ou superior, da infraestrutura da CONTRATANTE;

7. Permitir a integração com soluções de múltiplo-fator de autenticação, através dos protocolos OpenID e SAML 2.0;
8. Permitir a exportação de logs do sistema em tempo real para soluções de SIEM;
9. Permitir o envio de e-mails externos;
10. Permitir o sincronismo de horário por NTP e mostrar o relógio de acordo com os fuso-horários brasileiros;
11. A solução deve permitir a integração com outros sistemas através da importação de dados estruturados. A plataforma contratada deverá permitir a importação de dados, no mínimo, através dos seguintes métodos:
    1. arquivos CSV. Deverá permitir a importação de arquivos delimitados (CSV). Também deverá permitir a definição dos delimitadores de registros, de campos, de listas, além da possibilidade de definir sequências de “escapes”. A plataforma deverá permitir a definição da sequência numérica de registros que poderão ser ignorados durante a importação;
    2. arquivos XML ou JSON. Deverá permitir a importação de arquivos XML ou JSON e deverá permitir a utilização de definições XSLT, que possibilitam realizar transformações no arquivo XML/JSON original;
12. A solução deve permitir manter, renomear ou apagar os arquivos originais após o processamento de importação dos dados;
13. A solução deve estabelecer o mapeamento entre os campos originais e os campos específicos das aplicações da plataforma contratada, independentemente do método de transporte ou formato dos arquivos estruturados (CSV, TXT, XML, JSON, dentre outros);
14. A solução deve fornecer uma API (SOAP/REST/XML-RPC) para possibilitar a interação com aplicações externas. Esta API deverá ser disponibilizada, juntamente com a documentação, pelo fabricante da solução;
15. A solução deve permitir a integração com soluções de Business Intelligence e Data Visualization (Ex: PowerBi) por meio de uma API ou outra forma de integração para esse fim;

3.2. ESPECIFICAÇÕES MÍNIMAS DO MÓDULO DE LGPD:

1. Identificar, gerenciar, monitorar e analisar riscos dos tratamentos de dados da organização de forma integrada ao gerenciamento de riscos corporativos, de acordo com a norma brasileira de proteção de dados LGPD;
2. Criar e manter um inventário completo dos dados pessoais na organização (data-mapping), incluindo sua correlação entre ativos e processos de trabalho, com o apoio de formulários ou questionários de avaliação;
3. Permitir a localização e a correlação dos dados pessoais, dados pessoais sensíveis, ativos de informação, incidentes e riscos;
4. Criar e manter um inventário com os ativos de tecnologia da informação que tratem ou armazenem dados pessoais;
5. Permitir o desenho de fluxos de trabalho automatizados das avaliações de privacidade dos ativos e aplicações correlatas que utilizam dados pessoais;
6. Permitir armazenar informações acerca do ciclo de vida do tratamento de dados pessoais e os ativos (incluindo pessoas, base de dados, documentos, equipamentos, local físico, sistemas e unidades de negócio), no mínimo: coleta, retenção, processamento, compartilhamento e eliminação;
7. Permitir registrar a base legal para o tratamento de dados pessoais em cada processo mapeado;
8. Permitir a criação de relatórios e dashboards com as estatísticas de números de processos mapeados, quantidades de ativos, motivos de tratamento, etapas de tratamento e tipos de titulares de dados;
9. Permitir o registro de incidentes de segurança com dados pessoais;
10. Permitir vincular incidentes de segurança com dados pessoais aos riscos gerenciados e aos processos de tratamento;
11. Os modelos de gestão de riscos para os ativos de informação devem permitir a associação com no mínimo os seguintes controles: ISO 27001:2013, NIST V1.1, CIS Controls V8, através de modelos e processos pré-configurados;
12. Permitir a criação de questionários de avaliação para construir e implantar avaliações de privacidade para todas as jurisdições relevantes onde os dados privados estão armazenados.
13. Os questionários e formulários criados devem permitir a validação das respostas por um segundo usuário ou gestor;
14. Permitir executar avaliações de impacto de privacidade (PIA) e avaliações de impacto da proteção de dados (DPIA/RIDP), com geração de relatórios automatizada e customizável;
15. Permitir a criação de registros de riscos de tratamento atrelados aos ativos de informação, processos de tratamentos e controles de segurança;
16. Permitir parametrizar indicadores de performance para fins de monitoramento do desempenho e status de iniciativas de privacidade;
17. Permitir a emissão de relatórios de riscos gerenciados, ativos de informação, inventário de dados, incidentes e processos mapeados;
18. Permitir o acompanhamento dos processos que necessitam de gestão do consentimento (sem gerenciar diretamente o processo);
19. Permitir o acompanhamento e registro de solicitações de usuários (DSAR) para dúvidas, solicitações de dados pessoais, reclamações, etc, considerando um volume mínimo de 500 registros por mês, efetuados por usuários externos não nomeados;
20. Permitir a criação de dashboards customizáveis para gerenciamento;
21. Permitir a importação de formulários em formato XLS ou CSV que contenham: mapeamento de processos, riscos, ativos de informação, unidades organizacionais e quaisquer outras informações em lote que precisem ser cadastradas e estejam previamente disponíveis pela CONTRATANTE, que auxiliará na preparação e condensação das informações;
22. Permitir o cadastramento das unidades organizacionais/departamentos, com associação de localidade, endereço, e-mail, responsável e processos de tratamento de dados pessoais;
23. Permitir o cadastramento de fornecedores/operadores, com metodologia e avaliação de riscos integrada;
24. Permitir o gerenciamento de não-conformidades relativas aos processos de tratamento de dados pessoais;
25. Permitir o acompanhamento da conformidade e análise de riscos de fornecedores e terceiros, de forma integrada;
26. Permitir o gerenciamento de políticas de privacidade, riscos, controles e demais documentos que compõem o SGPI (Sistema de Gestão de Privacidade da Informação), de acordo com a norma ISO 27701:2019 e as boas práticas estabelecidas pela ANPD (Agência Nacional de Proteção de Dados Pessoais).

3.3. ESPECIFICAÇÕES MÍNIMAS DO MÓDULO DE GRC

1. Identificar, gerenciar, monitorar e analisar os riscos da organização, de forma integrada entre as várias unidades de negócio e grupos de trabalho;
2. Automatizar processos de conformidade e gerenciamento de riscos, de acordo com a norma ISO 31000:2018;
3. Permitir que a organização identifique, avalie e priorize riscos de maneira contínua e dinâmica;
4. Deve permitir, de forma geral, acompanhar e gerenciar o fluxo de trabalho (workflow) do processo de gestão de riscos, incluindo: a identificação de deficiências, a análise do risco, a avaliação quanto à tolerabilidade ao risco analisado, a proposição de ações de controle de risco e o monitoramento da efetividade desses controles;
5. Deve permitir utilizar as informações dos demais módulos para a gestão de riscos;

6. Possibilitar o registro dos Riscos identificados com, no mínimo, as seguintes informações:
    1. Nome do Risco, descrição, proprietário, stakeholders, gestor de risco, tipo ou categoria, status, direcionador, metodologia de avaliação do risco;
    2. Identificação do Risco Geral, incluindo os Riscos Inerente, Residual e Residual Calculado, tendências das probabilidades inerente e residual e tendências dos impactos inerente e residual;
    3. Pesquisa qualitativa, incluindo a probabilidade e impacto na ausência/existência de controles e transferência do risco;
    4. Pesquisa quantitativa, incluindo diversas categorias de risco, exposição e probabilidade considerando pior caso e caso típico, bem como a frequência de ocorrência sem controles e com controles;
    5. Definição de resposta e tratamento aos riscos, incluindo o tipo de resposta (aceitar, reduzir, evitar, compartilhar etc), status, descrição, data esperada para a resposta, além da identificação de possíveis controles mitigatórios;
    6. Associação dos riscos identificados a métricas (KRI), eventos de perdas, revisões trimestrais de risco e apontamentos;
    7. Definição de Níveis de Riscos Calculados;
    8. Permitir a realização de aprovações de riscos a partir de níveis previamente definidos;
    9. Associação com objetivos estratégicos do CONTRATANTE e seus processos de negócio.
7. Implementar a gestão de riscos de segurança da informação e privacidade, baseado nos controles dos frameworks ISO 27001:2013, ISO 27005:2019, ISO 27701:2019, NIST V1.1 e CIS Controls V8, com modelos, controles, dashboards, indicadores e relatórios específicos;
8. Implementar gestão de riscos TI (tecnologia da informação), baseado nas boas práticas de mercado (como COBIT, ITIL e ISO 20000-1:2011) com modelos, controles, dashboards, indicadores e relatórios específicos;
9. Implementar gestão de riscos ASG/ESG (ambiental, social e governança corporativa), com modelos, controles, dashboards, indicadores e relatórios específicos;
10. Implementar a gestão de continuidade de negócios, baseado na norma ISO 22.301: 2013, com modelos, controles, dashboards, indicadores e relatórios específicos;
11. Permitir a construção de mapas de calor com matrizes de tamanho e cores customizáveis;
12. Permitir a graduação da escala de probabilidades;
13. Permitir a criação de planos de tratamento de riscos, com atualização automática do risco residual;
14. Permitir a criação de modelos de riscos a partir dos quais possam ser criados novos riscos, que contenham no mínimo, processos, risco inerente, plano de tratamento, ativos e mapa de calor;
15. Permitir a inserção fórmulas e cálculos personalizáveis, sem a necessidade de desenvolvimento;
16. Permitir o agrupamento de riscos por categoria;
17. Permitir o agrupamento de riscos por nível de criticidade;
18. Permitir o agrupamento de riscos por estrutura de controle (frameworks e normas);
19. Permitir a revisão periódica e programada dos riscos, inclusive utilizando questionários e formulários;
20. Permitir a automação do levantamento de riscos através de questionários e formulários;
21. Permitir a elaboração e o envio agendado de relatórios;
22. Permitir a customização de dashboards;
23. Permitir a customização de relatórios;
24. Permitir gerar ciclo de vida de normativos e políticas de conformidade;
25. Permitir anexação de documentos em diversos formatos;
26. Permitir a criação de biblioteca com modelos de riscos, vulnerabilidades e ameaças, que possam ser utilizados na instanciação de novos riscos;
27. Permitir a criação de processos de auditoria/fiscalizações/testes sobre os riscos ou controles;
28. Permitir a granularização das permissões dos usuários para criação, alteração, exclusão e visualização de objetos, como riscos, relatórios, processos, dashboards, questionários e formulários;
29. Permitir a exportação de objetos em modo PDF e CSV;
30. Permitir o acesso de usuários externos, para acesso ao formulário de requisições (DSAR), sem a cobrança de licenciamento por usuário ou por acesso;
31. Permitir a visualização de dashboards, relatórios e resposta a formulários para usuários não nominados, assim como para usuários externos (operadores e fornecedores);
32. Permitir auditoria em todas as atividades de usuários, através de logs não apagáveis.

3.2. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

1. O TRE-ES possuirá independência tecnológica de operacionalização (haverá documentação de toda a solução e repasse de conhecimento).

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

1. Foram analisadas algumas soluções de mercado, com diversas apresentações de fornecedores. Ao todo foram analisadas 8 soluções, sendo 3 com escopo de atuação bastante reduzido e 5 mais aderentes às necessidades apresentadas pelas áreas, que foram convidadas a avaliar, de forma conjunta, as soluções disponíveis;
2. A solução contratada deveria atender as peculiaridades da gestão de riscos de vários grupos de interesse;
3. As soluções analisadas são softwares para gerenciamento de processos de LGPD e GRC (gerenciamento de riscos e conformidade), que poderão ser utilizadas para gestão dos processos de tratamentos de dados pessoais (LGPD);
4. Embora o licenciamento perpétuo poderia apresentar um custo relativamente menor, não estavam incluídos o custo da infraestrutura interna e o suporte da equipe técnica interna. Desta forma, o mais adequado é que a contratação seguisse o modelo SaaS;
5. A maioria dos fornecedores mostrou-se apta a prestar o serviço neste modelo. As principais soluções consideradas foram: IBM OnePages, Interact SA RiskManager, Modulo RiskManager e OneTrust;
6. Como as soluções possuem níveis de automação e features diferentes, procuramos estabelecer requisitos comuns na maioria delas, embora não seja possível conhecer 100% dos requisitos de cada uma antecipadamente, devido à complexidade deste tipo de solução, alguns requisitos de negócio e de segurança podem não ser atendido por 100% das soluções.
7. Estimativas para cada sistema:
    1. IBM OnePages - R$ 1.585.279,22;

2. Interact SA RiskManager - R$ 534.692,00;
3. Modulo RiskManager - R$ 452.500,00;
4. On Trust - R$ 800.000,00

8. Contratações Públicas Similares: Tribunal Regional do Trabalho da 8ª Região - TRT8 - Contrato TRT nº 9/2020 - Item - Software como serviço (SaaS) para Gestão de Riscos Institucionais (R$ 4.750,00/mês) + Item - Treinamento (R$ 1.850,00/pessoa).

5. INDICAÇÃO DA STIC ESCOLHIDA

5.1. DESCRIÇÃO DA SOLUÇÃO

1. Solução de Software para Gerenciamento de Processos de LGPD e Gerenciamento de Riscos e Conformidade (GRC), disponibilizada como serviço em nuvem pública (SaaS);

2. Dentre as opções de mercado, optamos pela solução de Software as a Service (SaaS), por ser a opção mais viável para a gestão da infraestrutura. Sendo assim, as propostas foram para esse tipo de serviço e o valor estimado para a contratação ficou em R$ 635.118,40 (seiscentos e trinta e cinco mil, cento e dezoito Reais e quarenta centavos) para o período de 12 meses. Quando da renovação, haverá a necessidade de renovação apenas do item 1.

5.2. JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

1. Optou-se pela contratação em item único devido às grandes diferenças nos modelos de licenciamento dos fabricantes, que podem necessitar de serviços diferentes para configuração, além de diversos módulos de software para atender aos requisitos da solução. Desta forma diminui-se os riscos da contratação para a Contratante.
2. Não localizamos, no âmbito da administração pública federal, licitação de solução equivalente nos últimos 02 anos, devido principalmente, ao surgimento recente da Lei Geral de Proteção de Dados. Assim, optou-se pela contratação de uma solução integrada no modelo SaaS.

5.3. ESTIMATIVA DE CUSTO

Grupo	ITEM	QUANT	ESPECIFICAÇÃO	VALOR UNITÁRIO				
				Módulo (2)	Interact Solutions	TRT8 (1)	Valor médio unitário (3)	Valor Total
	1	1	Solução de Software para Gestão de LGPD e Gestão de Riscos e Conformidade (GRC), por ano de uso	R$ 29.000,00/mês	R$ 51.961,41/mês	R$ 4.750,00/mês	R$40.480,70	R$485.768,4
	2	1	Consultoria para parametrização do sistema e implantação	R$96.000,00	R$143.000,00	R$0,00	R$119.500,00	R$119.500,0
	3	1	Workshop remoto	R$8.500,00	R$51.200,00	R$ 1.850,00/pessoa	R$29.850,00	R$29.850,00
	TOTAIS							R$635.118,4

(1) A contratação do TRT8 não previa LGPD e consultoria, ou seja, incompleta para os objetos dessa contratação. O valor para capacitação previa apenas 15 pessoas. Esta contratação prevê a capacitação de todos os envolvidos, um número muito maior. Portanto, não será considerada no cálculo.
(2) A proposta da empresa Módulo é de 2021, obtida pelo TRE-PR.
(3) O valor medido unitário foi obtido através da média dos orçamentos das empresas Módulo e Interact Solutions.
(4) O valor encontrado para a contratação ficou em R$ 635.118,40 (seiscentos e trinta e cinco mil, cento e dezoito Reais e quarenta centavos) para o período de 12 meses. Quando da renovação, haverá a necessidade de renovação apenas do item 1.

5.4. RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

1. Permitir quantidade de usuários ilimitada ou, no mínimo:
    1. 05 usuários com perfil de administrador -Permissão completa para configurações técnicas da solução. Serão utilizados pelos administradores da solução;
    2. 300 usuários com perfil de gestor de negócio (riscos e privacidade) – Permissão para gestão de riscos e privacidade, criação e alteração de dashboards, relatórios, modelos, testes, workflows e demais funcionalidades da solução. Serão utilizados pelos gestores de riscos definidos pela Política de Gestão de Riscos do TRE-ES;
    3. 312 usuários com perfil simplificado (riscos e privacidade – Permissão para avaliações (*survey*), na resposta a perguntas periódicas automatizadas, através de formulários predefinidos e configurados por um administrador ou usuário de Negócios. Acessar os objetos de Gestão de Políticas para fins de leitura, atestar e confirmar a leitura da política. Serão utilizados por demais colaboradores e fornecedores externos;
2. A demanda inicialmente previa a contratação de uma solução de software com licença perpétua, ou seja, que o TRE-ES seria proprietário da solução, podendo apresentar um custo relativamente menor. Mas, não estavam incluídos o custo da infraestrutura interna e o suporte da equipe técnica interna. Desta forma, o mais adequado é que a contratação siga o modelo SaaS. A maioria dos fornecedores mostrou-se apta a prestar o serviço neste modelo.

6. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

1. Não será necessária nenhuma adequação do ambiente, visto que se trata de contratação no modelo SaaS.

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. IDENTIFICAÇÃO DOS RISCOS

7.1. A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

	Risco	**Categoria**	**Probabilidade (P)**	**Impacto (I)**	**Nível do risco (P x I)**

ID					
R1	Não aprovação dos artefatos do planejamento da contratação	Contratação	Baixo	Médio	Baixo
R2	Atraso na tramitação do processo ou suspensão do certame em função de impugnações	Contratação	Baixo	Alto	Médio
R3	Orçamento insuficiente para a contratação	Contratação	Baixo	Alto	Médio
R4	Licitação deserta	Contratação	Baixo	Alto	Médio
R5	Solução sem adequação aos processos de gestão de riscos e cultura organizacional	Gestão	Médio	Baixo	Baixo
R6	Solução com preço exagerado que não permite o suporte em longo prazo	Gestão	Médio	Baixo	Médio

8. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

8.1. ANÁLISE DOS RISCOS

R1	RISCO: Não aprovação dos artefatos do planejamento da contratação			
	Probabilidade	Baixa	ID	Dano potencial
	Impacto	Médio	1	Atraso no processo de contratação
	ID	Responsável		Ação preventiva
	1	Equipe de planejamento		Reuniões com os envolvidos na contratação e com autoridades superiores para alinhamento, sensibilização e aprovação.
	ID	Responsável		Ação de contingência
	1	Equipe de planejamento		Ajustes necessários nos artefatos para encaminhamento do processo.

R2	RISCO: Atraso na tramitação do processo ou suspensão do certame em função de impugnações			
	Probabilidade	Baixa	ID	Dano potencial
	Impacto	Alto	1	Atraso na implantação da solução de GRC + LGPD.
	ID	Responsável		Ação preventiva
	1	Equipe de planejamento		Monitoramento do trâmite do processo nas unidades internas do TRE-ES
	2	Equipe de planejamento		Definição dos critérios de avaliação com respaldo na jurisprudência dos órgãos de controle
	ID	Responsável		Ação de contingência
	1	Equipe de planejamento		Resposta aos pedidos de impugnação em conjunto com assessoria jurídica e pregoeiro

R3	RISCO: Orçamento insuficiente para a contratação			
	Probabilidade	Baixa	ID	Dano potencial
	Impacto	Alto	1	Comprometimento da contratação
	ID	Responsável		Ação preventiva
	1	Equipe de planejamento		Repassar com a maior antecedência possível o estudo dos custos realizados.
	ID	Responsável		Ação de contingência
	1	Equipe de planejamento		Não havendo orçamento suficiente, rever o planejamento e reduzir o escopo da contratação.

R4	RISCO: Licitação deserta			
	Probabilidade	Baixa	ID	Dano potencial
	Impacto	Alto	1	Atraso no processo de contratação
	ID	Responsável		Ação preventiva
	1	Equipe de planejamento		Validar junto ao mercado as condições da contratação para evitar itens que reduzam a concorrência
	ID	Responsável		Ação de contingência
	1	Equipe de planejamento		Rever as exigências e republicar o edital.

R5	RISCO: Solução sem adequação aos processos de gestão de riscos e cultura organizacional			
	Probabilidade	Média	ID	Dano potencial
	Impacto	Baixo	1	Não atender ao objetivo da contratação
	ID	Responsável		Ação preventiva
	1	a designar		Apresentação da solução e discussão no Comitê Gestor de Proteção de Dados Pessoais

R6	RISCO: Solução com preço exagerado que não permite o suporte em longo prazo			
	Probabilidade	Média	ID	Dano potencial
	Impacto	Baixo	1	Não permitir o suporte no longo prazo
	ID	Responsável		Ação preventiva
	1			Forte atuação junto aos fornecedores para conhecer as soluções e suas *features*. A escolha do modelo da licitação também faz parte da estratégia de implementação faseada e formação de preço para conhecer o custo em longo prazo

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].

9. RECURSOS MATERIAIS E HUMANOS

1. Todos os Recursos Materiais necessários para a implantação deverão ser fornecidos pela empresa contratada. Em relação aos Recursos Humanos, será necessário a designação de equipe de fiscalização de contrato nos moldes previstos na Resolução TRE/ES n. 261/2018.

10. DESCONTINUIDADE DO FORNECIMENTO

1. A descontinuidade do fornecimento de atualização irá causar impacto imediato no TRE-ES. Sendo necessária nova contratação para que realize a mesma função para o Tribunal;
2. Em caso de necessidade de transição contratual, será necessária a aquisição/implantação de nova solução com funcionalidade igual ou superior.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria DG nº 216, documento 0635331)

Integrante Demandante: DARCY HENRIQUE ROCHA PELISSARI (substituto: THOMAZ CHEIM FIGUEIREDO)

Integrante Técnico: THIAGO NUNES DE ALBUQUERQUE SANTOS (substituto: BUENO BORGES DE SOUZA)

Integrante Administrativo: JOSE ADRIANI BRUNELLI DESTEFFANI (substituto: CARLOS ALBERTO DA ROCHA PADUA FILHO)

Vitória, 19 de setembro de 2022.

Documento assinado eletronicamente por **JOSE ADRIANI BRUNELLI DESTEFFANI**, **Secretário(a)**, em 23/09/2022, às 16:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DARCY HENRIQUE ROCHA PELISSARI**, **Analista Judiciário**, em 23/09/2022, às 16:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BUENO BORGES DE SOUZA**, **Analista Judiciário**, em 23/09/2022, às 16:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0813588** e o código CRC **70A97213**.