TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
R. Desembargador Leão Neto do Carmo, 23 - Bairro Parque dos Poderes - CEP 79037-100 - Campo Grande - MS

ESTUDO PRELIMINAR

1 ESTUDOS PRELIMINARES

1.1 SOLUÇÃO DE TI A CONTRATAR

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

1.2 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação é composta pelos seguintes membros:

Nome	Lotação	Tipo	Email
Jorge Luiz Batista Antônio	DG/AEDG	Demandante	jorge.antonio@tre-ms.jus.br
Marcelo Silva de Novaes	STI/COINF	Técnico	marcelo.novaes@tre-ms.jus.br
Graziela Gonçalves Silva Jurado	SAF/CRM/SLC	Administrativo	graziela.goncalves@tre-ms.jus.br

1.3 NECESSIDADE DA CONTRATAÇÃO

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. 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, entre outros, podendo ser utilizado pela alta gestão no monitoramento mais efetivo e no acompanhamento dos resultados.

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 ANÁLISE DA VIABILIDADE DA CONTRATAÇÃO (ART.14)

2.1 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA DEMANDA (ART. 14, I)

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

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 Mato Grosso do Sul 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 Tribunal Regional Eleitoral do Mato Grosso do Sul 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.

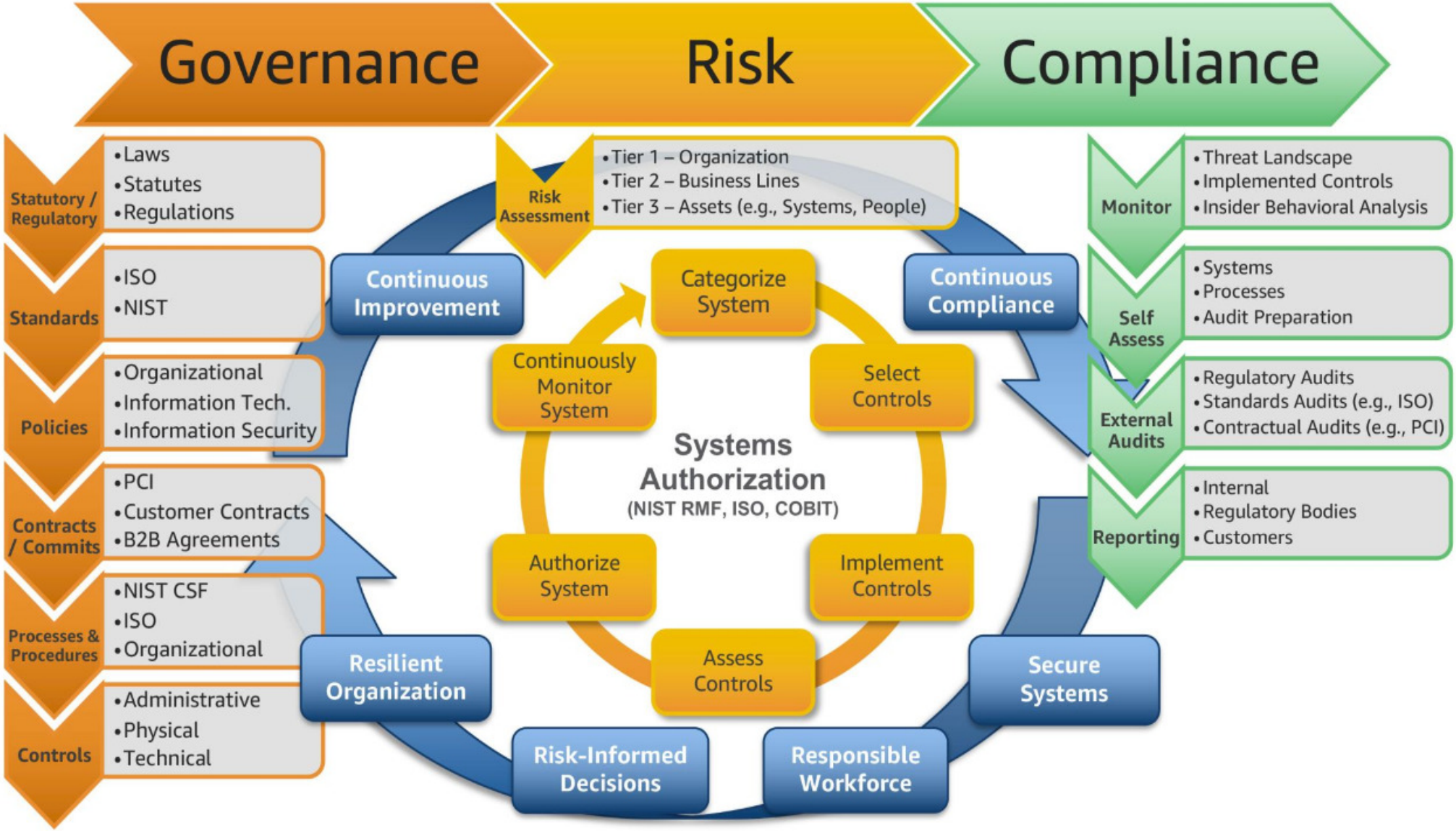
Considerações gerais sobre a solução:

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).
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 iniciais.
3. A solução de software deve ser de mercado, pronta e operacional, não sendo admitido soluções criadas especificamente para esta contratação.
4. A CONTRATADA declara 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.

Item 01 – Solução de software para gestão de LGPD e gestão de Riscos e Conformidade (GRC)

1. 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.
2. A solução de software deve ser capaz de fazer a gestão de riscos e conformidade, de acordo com os requisitos técnicos constantes neste edital.
3. O módulo de LGPD deve ser 100 % integrado ao módulo de GRC.
4. 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.
5. A quantidade mínima de usuários com perfil para gestão de processos de privacidade (LGPD) e gestão de riscos e conformidade (GRC) deve ser ilimitada, ou contemplar no mínimo: 05 usuários administradores, 300 usuários gestores de riscos e LGPD, 300 usuários externos.
6. Caso a solução leve em conta o número de funcionários do CONTRATANTE para o nível de licenciamento, deve considerar 700.
7. Deverá permitir a atualização para novas versões, consertos de falhas operacionais, conserto de vulnerabilidades de segurança e suporte técnico especializado.
8. 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.
9. A proposta deve incluir treinamentos para uso e administração da solução.

ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO:



1. **Especificações 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 forneceruma 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;

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. **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.

4. **Da quantidade e do tipo dos usuários:**
    1. Permitir quantidade de usuários ilimitada ou, no mínimo:
    2. 05 usuários com perfil de administrador -Permissão completa para configurações técnicas da solução. Serão utilizados pelos administradores da solução.
    3. 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 risocs definidos pela Política de Gestão de Riscos do TRE-MS (Resolução nº 657/2019).
    4. 300 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.
5. **Da configuração inicial e da disponibilização dos serviços:**
    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.
6. **Dos treinamentos para uso da solução:**
    1. A CONTRATADA deverá apresentar plano de treinamento para todos os usuários da solução, englobando LGPD, GRC e administração.

2.1.1 Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

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.

A solução contratada deveria atender as peculiaridades da gestão de riscos de vários grupos de interesse.

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),

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.

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.

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.

- IBM OnePages - R$ 1.585.279,22

- Interact SA RiskManager - R$ 534.692,00

- Modulo RiskManager - R$ 452.500,00

- On Trust - R$ 800.000,00

2.1.2 Contratações Públicas Similares (art. 14, I, b)

- 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).

2.2 IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES DE TIC (ART. 14, II)

Não se aplica, por se tratar de contratação de suporte oferecido apenas pelo fabricante da solução.

2.2.1 Disponibilidade de STIC similar em outro órgão (Art. 14, II, a)

Não se aplica, por se tratar de contratação de suporte oferecido apenas pelo fabricante da solução.

2.2.2 STIC existente no Portal de Software Público Brasileiro (Art. 14, II, b)

Não se aplica, por se tratar de contratação de suporte oferecido apenas pelo fabricante da solução.

2.2.3 A capacidade e as alternativas do mercado de TIC (Art. 14, II, c)

Não se aplica, uma vez que não existe nenhum órgão público, de qualquer esfera, que forneça o suporte solicitado nesse estudo.

2.2.4 Observância ao Modelo Nacional de Interoperabilidade (Art. 14, II, d)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida é referente a suporte a solução de hardware/software.

2.2.5 Aderência às regulamentações da ICP-Brasil (Art. 14, II, e)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida é referente a suporte a solução de hardware/software.

2.2.6 Observância ao Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) (Art. 14, II, f)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida é referente a suporte a solução de hardware/software.

2.2.7 Orçamento estimado (Art. 14, II, g)

Grupo	ITEM	QUANT	ESPECIFICAÇÃO	VALOR UNITÁRIO				
				Módulo **(2)**	Interact Solutions	TRT8 **(1)**	Valor médo unitário **(3)**	Valor Total
1	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$ 485.768,40
	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$ 119.500,00
	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$ 635.118,40

(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. Foi solicitada uma proposta atualizada para o TRE-MS, mas não foi enviada. Mas, utilizaremos para compor o cálculo.

(3) O valor médido unitário foi obtido através da média dos orçamentos das empresas Módulo e Interact Solutions.

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.

2.3 ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DAS STICs (ART. 14, III)

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.

2.4 DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA (ART. 14, IV)

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.

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.

2.4.1 DESCRIÇÃO DA SOLUÇÃO (ART. 14 IV, A)

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

2.4.2 ALINHAMENTO DA SOLUÇÃO (ART. 14, IV, B)

A Solução escolhida atende às necessidades do Órgão quando contribui para atender às necessidades de TI, uma vez que melhora o indicador: “Segurança da informação, infraestrutura de processamento e aplicativos”, constante do PETI do TRE-MS.

2.4.3 BENEFÍCIOS ESPERADOS (ART. 14, IV, C)

- Automação da gestão de tratamento de dados pessoais;
- Registro de incidentes, reclamações, compartilhamentos e riscos envolvendo dados pessoais, em consonância com a LGPD e as diretrizes da ANPD;
- Melhoria nos processos de gestão de riscos corporativos;
- Apoio na implementação do Plano de Continuidade de Negócios;
- Apoio na implementação de controles de Segurança da Informação;
- Apoio no monitoramento de indicadores de governança ambiental (ESG);

2.4.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA (ART. 14, IV, D)

A demanda prevista inicialmente previa a contratação de uma solução de software com licença perpétua, ou seja, que o TRE-MS 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 seguisse o modelo SaaS. A maioria dos fornecedores mostrou-se apta a prestar o serviço neste modelo.

2.5 ADEQUAÇÃO DO AMBIENTE (ART. 14, V, A, B, C, D, E, F)

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

3 SUSTENTAÇÃO DO CONTRATO (ART. 15)

3.1 RECURSOS MATERIAIS E HUMANOS (ART. 15, I)

Todos os Recursos Materiais necessários para a implantação deverão ser fornecidos pela empresa contratada.

Em relação aos Recursos Humanos, serão necessários:

- 02 (dois) servidores do quadro para atuarem como fiscais do contrato.

3.2 DESCONTINUIDADE DO FORNECIMENTO (ART. 15, II)

A descontinuidade do fornecimento de atualização irá causar impacto imediato no TRE-MS. Sendo necessária nova contratação para que realize a mesma função para o TRE-MS.

3.3 TRANSIÇÃO CONTRATUAL (ART. 15, III, A, B, C, D, E)

Em caso de necessidade de transição contratual, será necessária a aquisição/implantação de nova solução com funcionalidade igual ou superior.

3.4 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA (ART. 15, IV, A, B)

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

4 ESTRATÉGIA PARA A CONTRATAÇÃO (ART. 16)

4.1 NATUREZA DO OBJETO (ART. 16, I)

Trata-se de contratação de software, cujo uso é comum a diversas instituições da Administração Pública Federal, sendo padrão de mercado.

4.2 PARCELAMENTO DO OBJETO (ART. 16, II)

O objeto será composto por três itens que são parte de uma única solução e que, portanto, deverão ser fornecidos pela mesma empresa.

4.3 ADJUDICAÇÃO DO OBJETO (ART. 16, III)

A adjudicação do objeto será feita por lote único, tendo em vista que os itens do lote compõem uma solução global, interdependente e indivisível.

4.4 MODALIDADE E TIPO DE LICITAÇÃO (ART. 16, IV)

Após realização dos estudos técnicos chegou-se ao quantitativo de uma unidade para cada um dos três itens que compõem o grupo, por se tratarem os itens 2 e 3 de serviços de implementação e treinamento do software (Item 1).

Registra-se que o agrupamento não está em desacordo com o entendimento do TCU na Súmula 247, já que, por se tratar de serviços de implantação e treinamento do software que a mesma empresa irá fornecer não fere a competitividade, tampouco aumenta o risco de contratação antieconômica ou ocorrência de jogo de planilha.

Adotar-se-á o Sistema de Registro dePreços para permitir a participação de outras entidades da administração pública federal, conforme autoriza o art. 3º, III, do Decreto nº 7892/2013 que regulamenta o Sistema de Registro de Preços:

> Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:
>
> I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
>
> II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
>
> III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
>
> IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

4.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA (ART. 16,V)

As despesas decorrentes do objeto desta licitação, serão custeadas com recursos recursos aprovados na Lei Orçamentária da União nº 14.303 de 21/01/2022, que estima a receita e fixa a despesa da União para o exercício financeiro 2022 (LOA), Unidade 14112 – TRE-MS, Ação: 20GP- Julgamento de Causas e Gestão Administrativa, Programa de Trabalho 02.122.033.20GP.0054, **JC GAJE e Segurança da Informação.** Elementos de Despesa: 33.90.39 – OUTROS SERVIÇOS DE TERCEIROS – PESSOA JURÍDICA e 33.90.40.06 ou 33.91.40.06 – LOCAÇÃO DE SOFTWARE, SUBSCRIÇÃO OU LICENCIAMENTO DE SOFTWARE.

As despesas que, eventualmente, venham a ocorrer no exercício de 2023 serão custeadas com recursos previstos na Proposta Orçamentária, que serão indicados oportunamente.

Este item poderá sofrer alteração pela COPEG, unidade responsável pela Informação quanto à reserva e enquadramento orçamentários para cobrir a despesa, e de sua compatibilização com a Lei Orçamentária Anual, Plano Plurianual e a Lei de Diretrizes Orçamentárias.

4.6 VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO (ART. 16, VI)

O período de vigência desta contratação será de 12 (doze) meses, podendo ser prorrogado até o limite de 60 meses.

4.7 EQUIPE DE APOIO À CONTRATAÇÃO (ART. 16, VII)

A equipe de apoio à contratação será composta pela mesma equipe do presente estudo preliminar constante do item 1.2 deste documento.

4.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (ART. 16, VIII)

As atribuições cabíveis à fiscalização administrativa podem ser desempenhadas pela fiscalização técnica, auxiliada, no que couber, pela Seção de Gestão de Contratos Administrativos.

5 ANÁLISE DE RISCOS

Em atendimento às disposições contidas no art. 17 da Resolução CNJ 182 e IN 04/2014, art. 13, incisos de I a VI, esta Equipe de Planejamento de Contratação apresenta a consolidação das informações relativas ao gerenciamento dos riscos da contratação, considerando a probabilidade de ocorrência do risco, seu dano e as ações preventivas e de contingência.

A análise de riscos permite a identificação, avaliação e gerenciamentos dos riscos relacionados à contratação. Os riscos analisados foram organizados em duas categorias:

• Riscos que possam comprometer o sucesso do processo de contratação.

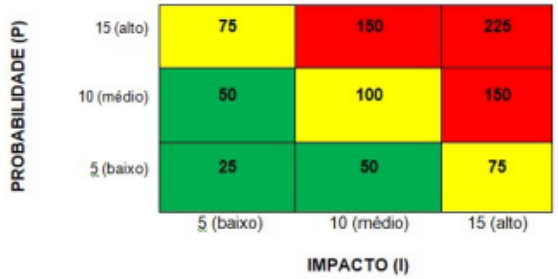
• Riscos de gestão ou de não atendimento das necessidades da Contratante.

Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos potenciais em caso de acontecimentos, possíveis ações preventivas e contingências, bem como a identificação de responsáveis por cada ação.

Após a identificação e classificação, deve-se executar uma análise qualitativa e quantitativa. A análise qualitativa dos riscos é realizada por meio da classificação escalar da probabilidade e do impacto, conforme a tabela de referência a seguir.

Classificação	Valor
Baixo	5
Médio	10
Alto	15

A análise quantitativa dos riscos consiste na classificação conforme a relação entre a probabilidade e o impacto, tal classificação resultará no nível do risco e direcionará as ações relacionadas aos riscos durante a fase de planejamento e gestão do contrato. A tabela a seguir apresenta a Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco.



O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz probabilidade x impacto. Caso o risco enquadre-se na região verde, seu nível de risco é entendido como baixo. Se estiver na região amarela, entende-se como médio. Já na região vermelha, entende-se como nível de risco alto.

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

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

• Riscos que possam comprometer o sucesso do processo de contratação.

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-MS
	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.

• Riscos de gestão ou de não atendimento das necessidades da Contratante.

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	Jorge Antônio		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	Jorge Antônio		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

6 DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

A equipe de planejamento, diante dos dados expostos, entende que a contratação é viável e necessária, uma vez que implantaremos uma solução de GRC e ficaremos conforme com a LGPD também.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Jorge Luiz Batista Antônio
AEDG - Integrante Demandante

Marcelo Silva de Novaes
COINF - Integrante Técnico

Graziela Gonçalves Silva Jurado
SLC - Integrante Administrativo

Documento assinado eletronicamente por **GRAZIELA GONÇALVES SILVA JURADO**, **Técnico Judiciário**, em 30/08/2022, às 19:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JORGE LUIZ BATISTA ANTONIO**, **Analista Judiciário**, em 31/08/2022, às 13:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCELO SILVA DE NOVAES**, **Coordenador(a)**, em 31/08/2022, às 13:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.app.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1087472** e o código CRC **B48E9C42**.