ROBSON CLEITON NOVAK:76303
18/06/2024 14:09

PAULO ROBERTO NUNES
18/06/2024 14:27

PAULO CELSO GERVA
20/06/2024 09:46

ESTUDOS TÉCNICOS PRELIMINARES PARA SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO

De acordo com o Guia de Contratações de TIC do Poder Judiciários, “o Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.”

“Fundamentação: além da legislação aplicável (Lei 14.133/2021), o presente estudo está em consonância com a Resolução CNJ 468/2022, alinhando-se ao Guia de Contratações de TIC do Poder Judiciário, na forma do art. 6º, Parágrafo único, da Res. CNJ 468/2022: “As contratações de STIC dos órgãos do Poder Judiciário seguirão a legislação vigente e observarão, na maior medida possível, as orientações dispostas no Guia estabelecido no art. 3º e as práticas e recomendações dos tribunais de contas.”

OBJETO: Contratação do módulo Cybersecurity Manager da plataforma Risk Manager, incluindo a migração de dados da licença perpétua do Risk Manager para nuvem (SaaS – software como serviço), treinamento e suporte técnico por 12 (doze) meses.

1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1 Descrição da necessidade da contratação:

O software Modulo Risk Manager é um software comumente conhecido como ‘solução GRC’, que trata de Governança, Riscos e Conformidade, e é utilizado pelo Tribunal Regional do Trabalho da 9ª Região desde agosto de 2015 para a realização de análises de risco do ambiente tecnológico, análises de conformidade com normas e resoluções, criação de planos de continuidade, acompanhamento dos incidentes de Segurança da Informação e acompanhamento dos controles de conformidade. O software ainda traz uma vasta base de conhecimento com as melhores práticas de segurança para os principais ativos tecnológicos, pessoas, ambientes e processos. É hoje uma ferramenta essencial para os trabalhos da Seção de Gestão de Segurança da Informação, inclusive sendo a base da gestão de riscos de ativos de tecnologia, do processo de trabalho de Gestão de Riscos de Tecnologia da Informação, da Secretaria Geral de Tecnologia da Informação e Comunicações.

Os fluxos de trabalho configurados no software também atendem demandas relacionadas à homologação de softwares, tendo como principal cliente a Coordenadoria de Gestão de Serviços de Tecnologia da Informação, CGSTI, e também aos registros de incidentes e eventos de segurança da informação associados à organização.

Ademais, com a publicação da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) pelo Conselho Nacional de Justiça, CNJ, através da Resolução Nº 396 de 07/06/2021, ficou clara a necessidade em alcançar a excelência em segurança cibernética no Poder Judiciário. Para tanto, faz-se necessária a aquisição de uma expansão da plataforma Risk Manager com a contratação do módulo Cybersecurity Manager.

Outrossim, considerando que hoje o software Risk Manager encontra-se instalado em infraestrutura local, dentro do Tribunal, requerendo constante esforço por parte da equipe técnica interna para manutenção, atualização e backup, tanto da base de dados como da máquina virtual que o hospeda, optou-se pela contratação da migração dos dados locais para nuvem da fabricante do software e a utilização da plataforma Risk Manager e o Cybersecurity Manager em nuvem (SaaS – software como serviço). Isso facilitará em muito a manutenção da solução, pois a responsabilidade de atualização do software ficará a cargo da fabricante, permitindo mais tempo do Tribunal para focar na operação da solução, que é foco da contratação em si. Além do mais, a expansão Cybersecurity Manager não funciona, nativamente, em ambiente local (*on premise*), sendo desenvolvida para acesso e operação em nuvem.

Acrescenta-se que será contratado também o treinamento tanto para o módulo de expansão como para a plataforma principal, visto que há o interesse interno da Coordenadoria de Governança de Segurança da Informação (CGSI) e SGTIC em ter mais pessoas capacitadas operando a solução, haja vista que hoje apenas uma pessoa é capaz de utilizar a ferramenta para criação dos projetos de análise de riscos, por exemplo.

Por fim, considerando os custos de soluções alternativas, e também os requisitos técnicos necessários, este estudo conclui pela continuidade da utilização do software Risk Manager (em uso atualmente pelo Tribunal). Apesar disso, conclui-se pela continuidade de uso do Risk Manager através de serviço online em nuvem, para que seja possível o uso do módulo Cybersecurity Manager. O uso do serviço online em nuvem terá contratação de acesso à plataforma por 12 meses, e engloba migração dos dados atuais do Tribunal. Como a fabricante do produto é a única que fornece o serviço de suporte, treinamento, e também a migração dos dados para nuvem, a contratação se dará por inexigibilidade.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, I: "I - descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público;" c/c Res. CSJT 364/2023, art. 33, I: "I – a descrição da necessidade da contratação, considerado o problema a ser resolvido;" Trata-se de elemento obrigatório do ETP, conforme o art. 18, § 2º, da Lei 14.133/2021, c/c art. 33 , § 1º da Res. CSJT 364/2023.

1.2 Descrição dos requisitos da contratação

Este estudo técnico visa descrever a necessidade de contratação de módulo de análise de riscos em cibersegurança, da plataforma Risk Manager; da contratação do suporte técnico por 12 (doze) meses e migração de dados da plataforma principal, que hoje é on

premise (local) para nuvem (SaaS – Software como Serviço) e da contratação de treinamento para o novo módulo de segurança cibernética e da plataforma principal, além contratação do serviço de parametrização e configuração do novo módulo.

Esta contratação tem como objetivo disponibilizar uma solução de gestão de riscos de segurança cibernética de forma que agregue ao trabalho da equipe técnica maior assertividade na análise de riscos, focando em controles de frameworks comuns ao mercado e que servem de base a auditorias e de órgãos superiores, como por exemplo. O framework CIS Controles versão 8. A eficácia, nesse sentido, poderá ser atingida com a contratação da expansão Cybersecurity Manager, da plataforma Risk Manager, o qual buscar resolver de forma eficiente a criação de projetos de análise de riscos de tecnologia, com painéis de evolução de fácil assimilação para ajudar a compreender o posicionamento do Tribunal na governança cibernética e nortear o caminho à melhoria contínua. A contratação de uma expansão para plataforma implica na contratação de serviço de configuração e parametrização do respectivo módulo contratado, visando deixa-lo preparado para o início dos trabalhos da equipe que irá operá-lo.

Considerando que o Tribunal possui licenças perpétuas do software de GRC (Governança, Riscos e Conformidade) Modulo Risk Manager e ele se encontra instalado em infraestrutura local, dentro do Tribunal, requerendo constante esforço por parte da equipe técnica interna para manutenção, atualização e backup, tanto da base de dados como da máquina virtual que o hospeda, com a migração de sua base de dados para versão em nuvem da plataforma, mantida pela fabricante, espera-se uma melhor eficiência no uso da ferramenta, pois não haverá mais a necessidade de manter uma ‘máquina virtual’ e toda infraestrutura associada para que o sistema opere localmente. O uso da plataforma em nuvem facilitará em muito a manutenção da solução, pois a responsabilidade de atualização do software ficará a cargo da fabricante, permitindo economia de tempo na manutenção da plataforma e direcionando esse tempo para operação da solução, que é o foco da contratação em si. Além do mais, a expansão Cybersecurity Manager não funciona, nativamente, em ambiente local (on premise), sendo desenvolvida para acesso e operação em nuvem.

Ademais, a contratação de treinamento tanto para a expansão Cybersecurity Manager como para a plataforma principal Risk Manager vai ao encontro da necessidade manter os recursos humanos preparados para a correta, eficiente e produtiva operação da solução. Como o último treinamento realizado da solução ocorreu na contratação de 2015, e atualmente apenas uma pessoa está capacitado para operar a plataforma principal Risk Manager, faz-se necessária a capacitação de mais pessoas, para que o Tribunal não dependa de apenas uma pessoa no que se refere a projetos de riscos de segurança da informação.

Visto se tratar de contratação de SaaS – Software como Serviço, em nuvem, o pagamento mensal da subscrição de acesso e uso já inclui a garantia da atualização técnica e atualização das bases de dados, bem como a abertura de chamados técnicos para a fabricante.

1.2.1 Requisitos de negócio

- Aprimorar a governança de TI;
- Aprimorar a gestão de segurança da informação e comunicações;
- Executar ações inerentes aos processos de governança, gestão de riscos e conformidade;
- Realizar periódicas e permanentes análises de risco e conformidade na área de Segurança da Informação e de Segurança Cibernética;
- Identificar e avaliar sistematicamente ameaças, vulnerabilidades em ativos baseadas em riscos e desconformidades a que estão expostos os processos de negócio suportados pela Tecnologia da Informação;
- Continuar a automatização e sistematização das ações e atividades inerentes aos processos de gestão de risco, governança e conformidade.
- Promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação.
- Manter o Sistema de Gestão em Segurança da Informação baseado em riscos, de acordo com recomendação do CNJ.
- Elaboração de Plano de Emergência, Crise, Continuidade do Negócio e Recuperação de Desastre a partir dos processos críticos e dos riscos.
- Estabelecer critérios que permitam monitorar e avaliar a execução da PSEC-PJ e de seus instrumentos, bem como o nível de maturidade em segurança da informação em cada órgão do Poder Judiciário.
- Elevar o nível de segurança das infraestruturas críticas, realizando, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos.

1.2.2 Requisitos técnicos

1.2.2.1 Requisitos gerais de funcionamento da solução

- Tanto o(s) software(s), como a infraestrutura de Nuvem pública e o suporte técnico deverão ser fornecidos pela CONTRATADA.
    - A solução deve estar armazenada e funcionar a partir da nuvem na modalidade Software as a Service (SaaS), sendo possível o acesso, a qualquer momento, dos usuários de qualquer local através de acesso web;
    - Deve estar hospedado em serviço na Nuvem de forma segura, com garantias de continuidade do serviço e recuperação de desastres;
- Permitir o acesso simultâneo de, no mínimo, 20 (vinte) usuários da organização;
    - As licenças fornecidas não devem ser nomeadas, permitindo assim o cadastro de um número ilimitado de usuários;
- Armazenar todas as senhas de usuários utilizando algoritmos de criptografia;
- Possuir módulo único e central de administração do ambiente, com controle de acesso por identificação e senha, cadastro de usuários, grupos e transações e definição de perfis de acesso, onde as permissões para cada uma das transações possam ser dadas diretamente ao usuário ou implicitamente através de um grupo do qual ele faça parte;

- Permitir a definição do nível de acesso, direitos e permissões de cada usuário ou grupo de usuários no sistema, a partir da definição de quais funcionalidades do software serão disponibilizadas, assim como as informações de cada um dos setores, permitindo o controle de acesso e registro de log de operações realizadas no sistema;
- Prover mecanismos de segregação de usuários através de nível de atuação (gestores de risco, auditores, gestores de conformidade, suporte, administração, etc);
- Permitir a granularidade das permissões dos usuários para criação, alteração, exclusão e visualização de objetos, como riscos, relatórios, processos, dashboards, questionários e formulários;
- Utilizar e apresentar mensagens e telas, em interfaces web, dashboards e relatórios, no idioma português do Brasil, sem customização ou instalação de recursos adicionais;
- Registrar as atividades em trilhas de auditoria mantendo o registro das alterações feitas nos dados e documentos com data, hora e usuário;
- Permitir auditoria em todas as atividades de usuários, através de registros de eventos não apagáveis;
- Registrar os acessos efetuados por todos os usuários em um arquivo de log, para fins de auditoria e elaboração de relatórios gerenciais. Esses dados serão acessíveis apenas por um grupo determinado de usuários autorizados, contendo no mínimo os seguintes dados: usuário, data, hora, transação realizada;
- Disponibilizar espaço de armazenamento de dados que garanta a boa performance do sistema e que seja compatível com a necessidade de utilização da CONTRATANTE, conforme a demanda, desde que dados e arquivos inseridos estejam de acordo com o escopo de utilização do software, podendo a CONTRATADA limitar o tamanho do upload a 25Mb por arquivo.
- Permitir a emissão de relatórios em formato PDF, Planilhas e CSV (Comma Separated Values);
- Permitir anexação de documentos em diversos formatos.
- Possibilitar uma interação dinâmica englobando Filtros, Filtros em cascata, Drill Down dentre outras opções, e exportação dos dados e resultados para, no mínimo, os formatos PDF, XLSX e imagem (PNG ou outros possíveis) gerados nos painéis e dashboards em todas as ferramentas, e módulos, que compõem a solução.
- Criar, de forma nativa na solução (diretamente pela interface), atributos personalizados para armazenamento de informações para os objetos que compõem o workflow de tratamento;
- Os atributos personalizados devem ser no mínimo das seguintes categorias: Anexo, Data/Hora, E-mail, Fórmula, HTML, Link, Lista de Opções, Número, Parágrafo e Texto;
- Disponibilizar documentação descrevendo os procedimentos de administração da solução (manual do módulo de administração) no idioma português do Brasil;
- Disponibilizar manual de utilização da solução (Manual do Usuário) no idioma português do Brasil;

- Disponibilizar documentação descrevendo os mecanismos que garantam o sigilo no tráfego e armazenamento de informações com o nível de criticidade que detenham, por exemplo criptografia de senha de usuário de banco de dados e credenciais de usuários administradores.

1.2.2.2 Requisitos do inventário de ativos

- Realizar cadastramento de ativos, viabilizando a elaboração de um inventário que contemple os elementos relevantes para as análises que serão realizadas pela organização;
- Fornecer diferentes formas de cadastrar ativos: em lote, por meio de planilhas; de forma automatizada, por meio de APIs; e de forma manual, por meio da própria interface;
- Personalizar e criar atributos para armazenar informações dos ativos de forma simplificada e diretamente pela interface do usuário;
    - Os atributos personalizados devem ser no mínimo das seguintes categorias: Anexo, Data/Hora, E-mail, Fórmula, Imagem, Link, Lista de Opções, Número, Parágrafo, Relacionamento, Texto e Tópicos;
- Visualizar a estrutura de ativos em formato de árvore segmentada, com possibilidade de estruturação tanto lógica quanto física;
- Segmentar de forma customizada e precisa o acesso às informações dos ativos, respeitando o princípio do privilégio mínimo e reduzindo possíveis impactos de acessos indevidos aos dados;
- Criar entrevistas web genéricas para preencher informações complementares e relacionadas aos ativos, incluindo atributos e propriedades nativas;
- Indicar revisores para as entrevistas web permitindo que outros usuários, com a permissão adequada, possam revisar e modificar as respostas dadas durante a entrevista, bem como inserir comentários em cada pergunta, maximizando a qualidade e a consistência das informações coletadas;
- Cadastrar Pessoas de forma manual e em lote através de planilhas;
- Cadastrar Pessoas de forma automatizada através do uso de integrações / APIs;
- Realizar integrações para importação de Pessoas/Objetos via LDAP e/ou Active Directory (AD), no mínimo;
- Estruturar um mapa de governança envolvendo, no mínimo, três níveis: Estratégico, Tático e Operacional, permitindo uma organização clara e eficiente das informações, além de auxiliar na tomada de decisão em diferentes níveis hierárquicos da organização;
- Interligar de forma intuitiva os componentes estratégicos, táticos e operacionais, proporcionando uma visualização clara e eficiente das relações entre eles;
- Realizar a interligação entre componentes de forma intuitiva pela interface ou em lote através de planilha, proporcionando flexibilidade e agilidade no processo de atualização;
- Apresentar consultas para extração/visualização dos dados de ativos, pessoas, árvore do inventário, níveis, dentre outros;
- Apresentar relatórios para os dados de ativos, pessoas, árvore do inventário, níveis, dentre outros;

- Apresentar painéis georreferenciados para extração/exibição de dados de ativos, pessoas, árvore do inventário, níveis, dentre outros;
- Possuir ferramenta para elaboração de Relatórios customizados pelos usuários para os dados de ativos, pessoas, árvore do inventário, níveis, dentre outros;
- Possuir ferramenta para elaboração e Dashboards customizados pelos usuários para os dados mencionados acima.

1.2.2.3 Requisitos de gestão de riscos em Segurança da Informação

- Criar projetos de Análise de Riscos, possibilitando que o seu escopo seja definido pelo autor, líder do projeto ou substituto;
- Adotar abordagem baseada em melhores práticas de mercado ao utilizar bases de conhecimento pré-definidas para análise de ativos, permitindo maior eficácia na gestão de riscos;
- Criar bases de conhecimento personalizadas diretamente pela interface, permitindo adequações das análises de risco em ativos de forma precisa, atendendo às particularidades do negócio;
- Parametrizar Ameaças, Fontes de ameaças, Agrupamentos de controles, CPEs e CCEs para serem relacionados a controles de bases de conhecimento;
- Adotar agentes de coleta automática para obter respostas aos controles das bases de conhecimento utilizadas nas análises de risco, possibilitando a otimização do processo de coleta de informações, garantindo a precisão e a confiabilidade dos dados;
- Utilizar múltiplos agentes de coleta, ampliando a abrangência e proporcionando um maior controle sobre a coleta de dados;
    - O agente de coleta deve ser independente e desacoplado da solução principal, permitindo a instalação em hardware separado para coleta de dados sem a obrigatoriedade de conexão em rede, oferecendo flexibilidade e autonomia para a gestão de riscos;
- Analisar riscos de segurança da informação, abrangendo minimamente os ativos de TI, ambientes, processos e pessoas, oferecendo uma visão abrangente e integrada da gestão de riscos;
- Disponibilizar questionários de análise de risco para ativos de tecnologia, atualizados para as versões mais recentes das tecnologias referências no mercado, de diversos fabricantes de sistemas e equipamentos, por exemplo, sistemas operacionais Windows e Linux em suas versões mais utilizadas e recentes, storages de dados, switches de rede, roteadores, virtualizadores etc;
- Analisar riscos associados a bases de conhecimento para outros tipos de ativos customizados que sejam necessários ampliação do entendimento do risco à segurança da informação.
- Identificar e avaliar riscos em diferentes níveis da organização;
- Criar entrevistas web para facilitar o preenchimento das respostas das bases de conhecimento (diretamente pela interface);
- Confeccionar regras nas entrevistas web para que a combinação de múltiplas respostas possa responder a um ou mais controles da base de conhecimento de forma dinâmica;

- Indicar revisores para as entrevistas web, estes devem possuir permissão para alterar as respostas e inserir comentários em cada pergunta;
- Gerar indicadores de Segurança, Riscos e Gap de controles de forma automática após a realização de análises de risco;
- Apresentar consultas para extração/exibição de dados contemplados nas análises de risco;
- Apresentar Relatórios Gerenciais para extração/exibição de dados contemplados nas análises de risco;
- Apresentar Relatórios Operacionais para extração/exibição de dados contemplados nas análises de risco;
- Apresentar painéis Georreferenciados para extração/exibição de dados contemplados nas análises de risco;
- Apresentar ferramental para elaboração de Relatórios customizados pelos usuários para extração/exibição de dados contemplados nas análises de risco;
- Apresentar ferramental para elaboração de Dashboards customizados pelos usuários para extração/exibição de dados contemplados nas análises de risco.
- Simular por meio de what-if o tratamento dos controles não implementados, possibilitando ao usuário uma observação das reduções nos níveis de riscos de acordo com suas escolhas para as implementações (simulação dinâmica e direta sem a necessidade de um projeto exclusivo para tal simulação);
- Replicar de forma completa um projeto de riscos (escopo, analistas e respostas);
- Comparar de forma automática os resultados de 02 (dois) ou mais projetos de análises de riscos de forma intuitiva através de painéis e interface do usuário;
- Gerar Indicadores de Riscos, Segurança e Gap de controles para as camadas Estratégica e Tática, baseada na análise da camada Operacional (ativos);
- Criar automaticamente um workflow de tratamento para os controles não implementados da seguinte forma:
    - Individual: uma ação para cada controle não implementado;
    - Agrupado por Plano de Ação: um plano de ação contendo várias ações filhas (controles não implementados);
    - Agrupamento único: uma única ação contemplando todos os controles não implementados;
- Alterar o fluxo do processo de aprovação e tratamento dos riscos de forma nativa (diretamente pela interface);
- Apresentar ferramental para elaboração de Relatórios customizados pelos usuários para extração/exibição de dados relacionados ao workflow de tratamento;
- Apresentar ferramental para elaboração de Dashboards customizados pelos usuários para extração/exibição de dados relacionados ao workflow de tratamento.
- Permitir a gestão de riscos baseada, obrigatoriamente, na norma ISO 31.000:2018 e, opcionalmente, nos frameworks COSO I e COSO II, para garantir uma terminologia e metodologia de acordo com as necessidades da organização.
- Possuir, no mínimo, em suas bases de conhecimento, documentos referenciais da ABNT NBR ISO/IEC 27002:2022, Critical Security Controls versão 8 (CIS v8) e Lei 13709/2018 (LGPD) para realização de análises de risco;

- 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;
- 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;
- Permitir a graduação da escala de probabilidades.
- Permitir a criação de planos de tratamento de riscos, com atualização automática do risco residual.
- Permitir a inserção fórmulas e cálculos personalizáveis, sem a necessidade de desenvolvimento.
- Permitir o agrupamento de riscos por categoria.
- Permitir o agrupamento de riscos por nível de criticidade.
- Permitir o agrupamento de riscos por estrutura de controle (frameworks e normas).
- Permitir a elaboração e o envio agendado de relatórios.
- Permitir a customização de dashboards de análise de riscos.
- Permitir a customização de relatórios.
- Permitir a criação de biblioteca com modelos de riscos, vulnerabilidades e ameaças, que possam ser utilizados na instanciação de novos riscos.

1.2.2.4 Requisitos de Gestão de Continuidade de Negócio

- Atender as Normas ISO 22301:2013 (Sistema de Gestão de Continuidade de Negócios -Requisitos) e ISO 22313:2015 (Sistemas de Gestão de Continuidade de Negócios -Orientações);
- Permitir a identificação dos processos críticos, a análise do impacto no negócio e qual o tempo que a organização suporta operar sem tais processos;
- Permitir a elaboração das Estratégias de Continuidade.
- Permitir a elaboração de Planos e Ações Operacionais;
- Permitir a elaboração de Plano de Emergência, Crise, Continuidade do Negócio e Recuperação de Desastre a partir dos processos críticos e dos riscos.

1.2.2.5 Requisitos de Gestão de Conformidade

- Permitir a avaliação de questões legais, como um normativo publicado, que possa vir a impactar o negócio do órgão, possibilitando o cadastro dos requisitos normativos e controle do nível conformidade;
- Permitir o desenvolvimento, manutenção e comunicação de políticas e procedimentos;
- Permitir a elaboração de questionário com perguntas para que o responsável do setor pontue quanto à conformidade ou não perante as perguntas. Para cada pergunta, além da conformidade, deve ser possível estabelecer a criticidade para

a pergunta, escrever um comentário e anexar evidências quanto à conformidade ou não do questionário;
- Permitir o estabelecimento de planos de ações, após as respostas do questionário, a fim de adequação das não conformidades identificadas, garantindo a realização de todo o acompanhamento até o devido atendimento legal;
- Permitir a definição dos requisitos de conformidade aplicáveis e acompanhar a sua implementação em tempo real para cada processo da unidade de negócio;
- Permitir o controle de revisões dos requisitos de conformidade;
- Permitir que cada programa de avaliação de conformidade tenha seus próprios critérios, respostas possíveis, pontuação e pesos;
- Possuir critérios de Classificação de Motricidade dos Fatores de Riscos/Não Conformidades, focando na priorização do tratamento ou anulação, evitando a materialização dos riscos.
- Permitir a análise de conformidade, para avaliar o nível de cumprimento dos requisitos;
- Permitir evidenciar eventos de não conformidade;
- Armazenar as consequências da não conformidade com os requisitos;
- Possuir a habilidade de criar tarefas ou atividades relacionadas à conformidade para monitorar a responsabilidade e o cumprimento das mesmas;
- Possuir a habilidade de relacionar requisitos externos aos programas de conformidade;
- Possuir, no mínimo, em suas bases de conhecimento, documentos referenciais da ABNT NBR ISO/IEC 27002:2022, Critical Security Controls versão 8 (CIS v8) e Lei 13709/2018 (LGPD) para realização de análises de conformidade.

1.2.2.6 Requisitos de Gestão de Segurança Cibernética

- Ter como referência os controles do Critical Security Controls versão 8 (CIS v8);
- Ter como referência o conjunto de normas ABNT ISO 27000 na versão mais recente disponível para cada normativo;
- Permitir a avaliação contínua de maturidade em cibersegurança, definindo linha de base e guardando a evolução continuada dos índices de cibersegurança da organização;
- Propiciar um ambiente adequado para gestão contínua de vulnerabilidades descobertas pela análise dos controles se segurança, através de avaliações, painéis e relatórios gerenciais e técnicos gerados pela solução;
- Permitir uma visão integrada da gestão de riscos cibernéticos tendo como referência valores e benefícios decorrentes das medidas de segurança implantadas;
- Disponibilizar ferramenta de simulação de mitigação de riscos, gerando estimativas de redução de índice de risco a partir da implementação de controles.

1.2.3 Requisitos de capacitação

- A CONTRATADA deverá apresentar plano de treinamento de todos os módulos/sistemas que compõem a solução.
- A execução dos serviços de treinamento se dará após emissão de ordem de serviço;
- O treinamento técnico terá como escopo todos módulos fornecidos na solução, cobrindo as áreas mínimas de: Gestão de Riscos em Segurança da Informação; Gestão de Cibersegurança;
- O treinamento deve ser fornecido para até 10 (dez) alunos e deverá ter duração mínima de 24 horas;
- O treinamento deverá ser, majoritariamente, na modalidade ONLINE, de modo síncrono.
- A CONTRATADA será responsável por disponibilizar o ambiente de ensino a distância, que permita aos alunos interagirem em tempo real com o instrutor para esclarecimento de dúvidas;
- O treinamento deverá ser ministrado em português, por técnico qualificado, e composto de aulas teóricas e práticas;
- A CONTRATADA deverá confeccionar e disponibilizar aos participantes todo o material didático necessário ao treinamento;
- A ementa e material utilizado no treinamento deverão ser enviados previamente ao Tribunal para avaliação e aprovação;
- Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso. As avaliações deverão ser preenchidas e assinadas pelos alunos e posteriormente entregues ao TRT9 para a assinatura do aceite do serviço de treinamento;
- Caso o treinamento seja avaliado como insatisfatório pela maioria dos participantes da turma, o treinamento deverá ser refeito;
- Será considerado insatisfatório o treinamento que obtiver maioria dos itens da avaliação de treinamento julgados como RUIM ou REGULAR, observadas todas as avaliações preenchidas;
- O treinamento a ser refeito por ocasião de ter sido mal avaliado não pode gerar novas despesas para a CONTRATANTE;
- Ao final do treinamento, cada participante deverá receber um certificado assinado pela CONTRATADA, contendo informações de data, carga horária, conteúdo ministrado, além do nome completo do instrutor, do aluno e da instituição que forneceu o curso, bem como o seu período.

1.2.4 Requisitos legais

- Atender às normas gerais de licitação e contratação para a Administração Pública contidas na Lei nº 14.133, de 1º de abril de 2021;
- Atender às diretrizes para contratações de Solução de Tecnologia da Informação e Comunicação contidas na Resolução do Conselho Nacional de Justiça (CNJ) Nº 468, de 15 de julho de 2022;

- Atender às diretrizes que disciplinam o exercício de cargos livre de nepotismo contidas na Resolução do Conselho Nacional de Justiça (CNJ) Nº 229, de 22 de junho de 2016, no qual determinada que a CONTRATADA deverá apresentar declaração informando não possuir em seu quadro societário - bem como entre seus gerentes e diretores - cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, ou servidor investido em cargo de direção e de assessoramento do Tribunal Regional do Trabalho da 9 Região;
- Atender às diretrizes contidas na Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD);
    - A CONTRATADA deverá realizar o tratamento de dados pessoais e dados pessoais sensíveis em nome do TRT da 9ª Região, nas as atividades que se fizerem necessárias para o cumprimento do Contrato, nos termos do inciso VII, do art. 5º e art. 39, da Lei nº. 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);
    - A CONTRATADA deverá cumprir as disposições da Lei nº 13.709, de 14 de agosto de 2018, implementando medidas técnicas e organizacionais adequadas para assegurar a proteção dos direitos do titular dos dados pessoais;
    - A CONTRATADA deverá conhecer, observar e respeitar todas as normas e políticas do TRT da 9ª Região que versem sobre o tratamento de dados pessoais e dados pessoais sensíveis, cumprindo o disposto na Política N° 55, de 29 de março de 2021, que estabelece diretrizes para a Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 9ª. Região. (fonte: https://www.trt9.jus.br/portal/arquivos/7606199).

1.2.5 Requisitos de manutenção

- Manter disponíveis os serviços contratados durante 24 horas, 7 dias por semana, 365 dias no ano, garantindo disponibilidade mensal do serviço de 99,9%;
    - Poderão ser desconsiderados para fins de apuração da disponibilidade mensal os seguintes eventos se atendidas as condicionantes:
        - Interrupções planejadas (se notificadas pela CONTRATADA com pelo menos 24 horas de antecedência através de e-mail, e se programadas para o período que vai de 06:00 PM [hora de Brasília] de dia útil, até às 07:00 AM [hora de Brasília] do dia útil subsequente);
        - Qualquer indisponibilidade causada por caso fortuito ou força maior, ações de governo, inundações, incêndios, terremotos, conflitos civis, atos de terrorismo, greves ou problemas laborais (exceto os que envolvem funcionários da CONTRATADA), falhas ou atrasos do fornecedor do serviço de Internet, desde que inequivocamente comprovadas;

- Prestar os serviços através de pessoal capacitado, para que os mesmos sejam prestados dentro de um padrão de qualidade e perfeição técnica exigível pelo mercado;
- Atualizar o ambiente de produção do TRT9 sem custos adicionais, em caso de publicação de nova versão do software;
- Realizar diariamente o backup dos dados do Tribunal e garantir a recuperação completa desses dados em caso de incidentes de segurança da informação.
- A Contratada deverá prestar serviço manutenção e suporte técnico destinado a:
    - Restabelecimento de serviços interrompidos ou degradados;
    - Solução de problemas de configuração e falhas técnicas nos serviços;
    - Esclarecimentos de dúvidas sobre configurações e utilização dos serviços;
    - Implementação de novas funcionalidades;
    - Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas (sem quaisquer ônus para o Contratante), no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados
- Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções disponibilizadas.

1.2.6 Requisitos temporais

- Prazo contratual de 12 (doze) meses, a contar da data assinatura do contrato, renovável por igual período para os itens 1 (um) e 2 (dois);

ITEM	DESCRIÇÃO DO ITEM	PRAZO
1	SaaS - Plataforma Risk Manager para nuvem.	Disponibilidade no acesso à plataforma em até 10 dias após a assinatura do contrato.
2	SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem.	Disponibilidade no acesso à plataforma em até 10 dias após a assinatura do contrato.
3	Migração de dados da licença perpétua do Risk Manager para nuvem.	Finalização da migração em até 30 dias após a assinatura do contrato.
4	Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.	Execução do treinamento em até 60 dias após a assinatura do contrato.
5	Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.	Término da prestação do serviço em até 90 dias após a assinatura do contrato.

1.2.7 Requisitos de segurança da informação

- A CONTRATADA deverá seguir todas as normas, políticas e procedimentos de segurança estabelecidas pelo contratante para execução do contrato, tanto nas dependências do contratante como externamente;

- Havendo documento padronizado, disponibilizado pelo TRT9, em meio eletrônico e/ou papel, que verse sobre segurança da informação, é importante que a CONTRATADA dê ciência e concorde plenamente com as premissas apontadas;
- A CONTRATADA deverá observar e respeitar, rigorosamente, todas as normas e procedimentos de segurança do TRT9, assim como as suas atualizações, cumprindo o disposto na Política de Segurança da Informação - PSI (RA 85) (https://www.trt9.jus.br/portal/arquivos/6774415);
- A CONTRATADA deverá manter sob sigilo, sob pena de responsabilidade civil, penal e administrativa, todo e qualquer assunto de interesse do Tribunal ou de terceiros de que tomar conhecimento em razão da prestação do serviço;
- Sem a autorização por escrito do CONTRATANTE, a CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude da entrega dos materiais, ou de que tenha tomado conhecimento em decorrência da execução do objeto;
- A CONTRATADA deve zelar para que todos os privilégios de acesso a sistemas, informação e qualquer outro recurso do contratante sejam utilizados exclusivamente na execução dos serviços e pelo tempo estritamente necessário;
- A CONTRATADA não poderá compartilhar dados pessoais com outras pessoas jurídicas ou físicas, salvo em caso obrigação legal ou com prévia autorização do TRT da 9ª Região;
- Nas hipóteses de compartilhamento previstas no item anterior, a CONTRATADA assume toda a responsabilidade decorrente, especialmente no que diz respeito à observância da adequada proteção e resguardo aos direitos dos titulares originais.

1.2.8 Requisitos sociais, ambientais e culturais

- Estar habilitada juridicamente (regularidade fiscal e trabalhista).
- Cumprir o disposto no inciso XXXIII do art. 7.º da Constituição Federal de 1988, quanto ao emprego de menores;
- Observar, no que couber, as diretrizes, critérios e práticas de sustentabilidade do Guia de Contratações Sustentáveis da Justiça do Trabalho, em sua 3ª Edição, aprovado pela Resolução do Conselho Nacional de Justiça (CNJ) nº 310, de 24 de setembro de 2021.

1.2.9 Requisitos de arquitetura tecnológica

- Disponibilizar acesso à solução de qualquer local através de acesso Web, a qualquer momento, por se tratar de solução SaaS - Software como Serviço;
- Deve ser 100% baseado em plataforma Web compativel com o padrão W3C;
- Permitir a integração com soluções de múltiplo-fator de autenticação (MFA), através dos protocolos OpenID e SAML 2.0;

- Permitir o envio de logs do sistema em tempo real para soluções de centralização de logs/SIEM;
- Possuir interface para monitoramento de notificações enviadas por e-mail;
- Permitir o envio de e-mails externos;
- Permitir o sincronismo de horário por NTP e mostrar o relógio de acordo com os fuso-horários brasileiros;
- Ser compatível pelo menos com os seguintes navegadores: Google Chrome, Mozilla Firefox e Microsoft Edge;
- Possuir interface responsiva que permita acesso das principais funções através de tablets e smartphones;
- Realizar comunicação segura entre os diferentes componentes da solução e com a estação de trabalho usando padrões de criptografia e protocolos, ambos não proprietários (Ex. SSL);
- Utilizar o protocolo HTTPS, com suporte a TLS 1.2 ou superior;
- Suportar mecanismo de autenticação única (Single Sign-On - SSO), de modo que os usuários possam efetuar logon na solução de GRC utilizando as mesmas credenciais da rede interna do Tribunal.
    - Esse mecanismo deverá ser nativo e configurável dentro da própria ferramenta, fazendo uso de padrões abertos de autorização (SAML/oAuth) ou possibilitando a sincronização automática dos usuários e senhas da solução de GRC (em nuvem) com o Active Directory (AD) da Microsoft localizado na rede interna (on premise) do Tribunal e em nuvem, caso seja necessário;
- Ser compatível com o Active Directory versão Windows Server 2012R2 e Windows Server 2016 (versões específicas do AD), instalado em servidores com o Sistema Operacional Windows Server 2016, 2019 e 2022.
- Permitir a criação e execução de rotinas de sincronização de objetos com o Active Directory, com importação de usuários e computadores (ativos de tecnologia), por exemplo;
- 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:
    - 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;
    - 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;
- Permitir 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);
- 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;

- 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;
- Permitir a expansão e integração total de todos os módulos da solução da fabricante que, porventura, vierem a ser adquiridos posteriormente, aproveitando em cada módulo os dados gerados em outro módulo qualquer da solução.

1.2.10 Requisitos de projeto e de implantação

- O CONTRATANTE disponibilizará acompanhamento para o acesso necessário e providenciará as condições imprescindíveis para a CONTRATADA efetuar a migração de dados e infraestrutura on premise da licença perpétua do software Modulo Risk Manager para plataforma em nuvem.
    - A migração envolverá não só a migração dos dados como também a migração/criação de fluxos de trabalho na plataforma em nuvem compatíveis com os criados de forma customizadas para o TRT9 e que hoje estão presentes na solução instalada localmente;
- A equipe que participará da Operação Assistida será indicada pelo CONTRATANTE, a qual trabalhara com a equipe da CONTRATADA para implantar e parametrizar a expansão Cybersecurity Manager contratada, podendo envolver a criação de novos fluxos de trabalho (workflows), painéis, relatórios etc específicos para a organização, definidos em comum acordo entre as partes e que não consuma quantidade maior de horas que o contratado.

1.2.11 Requisitos de garantia e manutenção

- Os serviços de suporte técnico serão solicitados mediante a abertura de chamado técnico via ligação telefônica (local ou gratuita) ou por meio eletrônico na internet (e-mail ou website), ao fabricante ou à empresa autorizada, em qualquer caso em português. O serviço de abertura e de atendimento de chamado deverá estar disponível em horário comercial (horário de Brasília/DF, das 8 às 18h, de segunda à sexta-feira), sem custos para o CONTRATANTE;
- Não haverá limitação de quantidade de abertura de chamados para suporte;
- Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá à contratada fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços;
- Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços;
- O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.
- Permitir a atualização para novas versões, consertos de falhas operacionais, conserto de vulnerabilidades de segurança e suporte técnico especializado de forma transparente para o CONTRATANTE;

- A CONTRATADA deverá cumprir os seguintes prazos de acordo com a severidade do evento:

Tabela de Atendimento		
Severidade	**Descrição**	**Prazo para início do atendimento**
Urgente	Funções críticas paradas ou com problemas que impactam significativamente o uso	Até 1 (uma) hora útil.
Normal	Problemas ou erros contornáveis, que não impactam significativamente o uso	Até 2 (duas) horas úteis.
Informações	Consulta Técnica, dúvidas em geral, monitoramento	Até 8 (oito horas) úteis.

- O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do chamado.
- O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do TRT9.

1.2.12 Requisitos de experiência da equipe de projeto, implantação e manutenção da solução

- A CONTRATADA deverá designar técnicos especializados na plataforma Risk Manager e a expansão Cybersecurity Manager, para migração dos dados da instalação local para nuvem da fabricante, para parametrização e configuração do módulo contratado e para o atendimento aos chamados criados, com a possibilidade de escalação de nível de serviço para técnicos mais especializados, caso o problema não seja resolvido em tempo hábil pelos técnicos do nível anterior.

1.2.13 Requisitos de formação da equipe de projeto, implantação e manutenção da solução

Não se aplica.

1.2.14 Requisitos de metodologia de trabalho

- A CONTRATADA deverá disponibilizar Relatório Gerencial de Chamados, sempre que requisitado pelo CONTRATANTE, que deverá conter a relação de todos os chamados técnicos ocorridos, contendo a informação de sua numeração, data e hora de abertura, tempo total decorrido desde a abertura até a solução definitiva e o nível de criticidade e as informações;

  - O Relatório Gerencial de Chamados pode ser fornecido através de consulta no histórico de chamados abertos na plataforma de abertura de chamados técnicos;
- A CONTRATANTE deverá disponibilizar servidor da área técnica para acompanhamento e assessoramento do técnico da CONTRATADA que providenciará a migração dos dados locais para nuvem;
- A CONTRATANTE deverá disponibilizar servidor, ou equipe técnica, da área que utilizará a ferramenta, para acompanhar e orientar o trabalho da Operação Assistida, durante uso da ferramenta em nuvem no período de tempo contratado.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, III: "III - requisitos da contratação;" c/c Res. CSJT 364/2023, art. 33, III: "III - requisitos da contratação, contendo, inclusive, critérios de sustentabilidade e acessibilidade, quando aplicáveis;".

1.3 Levantamento de mercado, consistente na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar - Soluções Disponíveis no Mercado de Tecnologia da Informação

Foram pesquisadas soluções na linha de atuação de software de GRC (Governança, Riscos e Conformidade), focando em Segurança Cibernética, sendo que as pesquisas foram realizadas levando em consideração requisitos descritos aderentes às funcionalidades hoje utilizadas no software GRC Risk Manager, da empresa Modulo Security Solutions S/A. Além da empresa Modulo, foram encontradas outras duas empresas que atuam fornecendo soluções de GRC: Interact Solutions e OneTrust, conforme detalhes registrados a seguir.

Foi enviada a lista de requisitos para a empresa nacional Interact Solutions (https://www.interactsolutions.com/), a qual fabrica e comercializa uma solução de GRC aderente a diversas metodologias do mercado. Porém, a resposta recebida do contato da Central de Negócios da Interact, após receber a lista de requisitos descritas nesse estudo, foi que de 'há uma lacuna nos quesitos específicos de riscos quando adentramos ao escopo de cibersegurança, continuidade de negócio e conformidades' quando comparados com a solução por eles fabricada, conforme arquivo '[*1] E-mail - Interact Solutions_ Resposta aos Requisitos.pdf*.' Portanto, a solução da empresa Interact não é totalmente aderente às necessidades requisitadas pelo TRT9.

Também foi encontrada a solução chamada OneTrust (https://www.onetrust.com/pt/), que, dentre as soluções em software em seu portfólio de produtos, está uma solução de GRC. Sendo assim, foi enviada a lista de requisitos para a empresa Trust4U (https://www.trust4u.com.br/), a qual comercializa a solução da OneTrust no Brasil.

Em reunião para apresentação do produto, foi salientado tanto pela fabricante como pela empresa que comercializa no Brasil, que a solução OneTrust tem uma abordagem diferente da abordagem de análise de riscos do Risk Manager, o qual define o grau de risco de ativos de tecnologia, ambiente, pessoas e processos através da verificação da existência e habilitação exaustiva de controles técnicos para determinado ativo. Ademais,

uma das funcionalidades utilizadas hoje, da Coleta Automática de respostas a controles de ativos de tecnologias, não está disponível na solução da OneTrust. Portanto, a solução da fabricante OneTrust, comercializada pela empresa Trust4U, também não é totalmente aderente às necessidades requisitadas pelo TRT9.

Como o TRT9 possui licenças perpétuas para o software instalado localmente, há a possibilidade de se continuar a utilizar a versão atualmente instalada na infraestrutura local, a qual está, por ora, funcional e em utilização para execução das análises de risco. Porém, considera-se essa opção inadequada pelos seguintes motivos:

- Não há suporte técnico contratado e todo problema com a solução e/ou com o servidor virtual no qual ela está instalada, como já ocorreu, deve ser resolvido somente pela equipe interna, onerando outras atividades da unidade;
- Não há atualização disponível para a solução nem para as bases de conhecimento nela instaladas;
- Não há a possibilidade de utilização da expansão Cybersecurity Manager da plataforma principal sem a migração dos dados para nuvem e sem o firmamento de novo contrato de aquisição, pois se trata de novo produto da fabricante Modulo Security Solutions S/A;
- É arriscado ao TRT9 continuar a depender de uma solução sem suporte nem atualização para desempenho de suas atividades relacionadas, principalmente, à gestão de riscos de segurança da informação, ainda mais nesse momento em que o processo de gestão de riscos de segurança da informação está atrelado à execução do processo de gestão de riscos de Tecnologia da Informação e Comunicação.

Sendo assim, considerando o não atendimento dos requisitos técnicos necessários pelos softwares alternativos das empresas Interact Solutions e OneTrust, este estudo técnico conclui pela continuidade da utilização do software Risk Manager da empresa Modulo Security utilizado até hoje pelo Tribunal, na versão de instalação local, on premise. Entretanto, devido aos 4 pontos detalhados acima no que se refere à criticidade da solução e à falta de suporte, de atualização e de expansão, não considera-se adequado a manutenção do uso da solução na infraestrutura instalada atualmente.

Portanto este estudo conclui pela contratação do módulo Cybersecurity Manager da plataforma Risk Manager através de serviço online (em nuvem), por 12 (doze) meses, incluindo a migração de dados do TRT9, treinamento e suporte técnico, conforme quadro detalhado a seguir. Adicionalmente entende-se tecnicamente necessário a contratação de 140 horas técnicas (o que equivale a 20 dias úteis, ou aproximadamente período de 1 mês) para que ocorra operação assistida pelo fabricante na implantação do módulo Cybersecurity Manager.

Importante enfatizar, que a empresa Módulo Security fabricante do produto Risk Manager possui atestado de exclusividade de prestação de serviços de suporte e garantia para a plataforma Risk Manager, conforme Certificado de Propriedade emitido pela FENAINFO. Desta forma indica-se a realização desta contratação através de inexigibilidade. Ambos estes detalhes também encontram-se registrados no item 3.3 deste estudo.

Abaixo detalha-se a proposta comercial recebida da empresa Módulo Security para a contratação do módulo Cybersecurity Manager da plataforma Risk Manager, incluindo a migração de dados da licença perpétua do Risk Manager para nuvem, treinamento e suporte técnico por 12 meses, e operação assistida de 140 horas.

LEVANTAMENTO DAS ALTERNATIVAS

Necessidade 1 – Manter em execução processos de gerenciamento de riscos e expandir o uso da ferramenta focando na análise e implantação de controles de segurança cibernética.
Solução Única – Contratação do módulo Cybersecurity Manager da plataforma Risk Manager, incluindo a migração de dados da licença perpétua do Risk Manager para nuvem (SaaS – software como serviço), treinamento e suporte técnico por 12 (doze) meses.

Proposta da Empresa **Modulo Security Solutions S/A**[1]

Descrição:	**Item 1** SaaS - Plataforma Risk Manager para nuvem	**Item 2** SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem	**Item 3** Migração de dados da licença perpétua do Risk Manager para nuvem.	**Item 4** Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.	**Item 5** Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.
Valor Proposto (Mensal):	R$ 3.600,00	R$ 2.500,00	---	---	----
Valor Proposto (Anual):	R$ 43.200,00	R$ 30.000,00	R$ 18.000,00	R$ 10.000,00	R$ 25.200,00
Orçamento Estimado (Anual):			**R$ 126.400,00**		

1.3.1 Contratações públicas similares

[1] Conforme informações comerciais encontradas no arquivo "[2] Proposta Comercial TRT 9a Expansão da Plataforma Risk Manager.pdf"

A pesquisa de preços foi realizada nos sites **Painel de Preços, Compras Governamentais, Diário Oficial da União e Sollicita**.

Foram encontradas 3 contratações por inexigibilidade de licitação, todas do software Risk Manager fornecido pela a empresa Módulo Security. Com base nos valores encontrados, pode-se verificar que a proposta comercial recebida pelo TRT9 encontra-se com valor compatível com o encontrado em contratos recentes, inclusive sendo menor dos valores dentre as outras contratações similares encontradas.

Contrato 1			
	Órgão / Instituição:	Agência Nacional de Vigilância Sanitária – ANVISA	
	Instrumento Contratual:	Primeiro Termo Aditivo do Contrato nº 14/2020	
	Contratada:	Modulo Security Solutions	
	Objeto:	Contratação de serviços de Suporte Técnico ao Software Módulo Risk Manager com atualização de versão, tendo como objetivo manter a solução sempre atualizada e em pleno funcionamento.	
	Vigência:	24 meses (2024)	
	Modalidade do Serviço:	*On-premise* (licença perpétua)	
	Tipo da Contratação:	**Inexigibilidade de Licitação**	
	Arquivo:	[5.3] ANVISA - 1o Termo Aditivo do Contrato 14-2020 - Plataforma GRC Modulo.pdf	
	Item	**Descrição do Item**	**Valor Unitário**
	1	Sustentação de Software	R$ 880.000,00
		Valor Total do Contrato	R$ 880.000,00
		Valor Anual	**R$ 440.000,00**

Contrato 2			
	Órgão / Instituição:	Comando do Exército – Comando de Comunicações e Guerra Eletrônica do Exército – CCOMGEX	
	Instrumento Contratual:	Contrato nº 07/2023	
	Contratada:	Modulo Security Solutions	
	Objeto:	Contratação do Suporte, Manutenção e Atualização de Licença do Software de Governança. Risco e Conformidade (GRC) Risk Manager, com Garantia Técnica, pelo período de 12 (doze) meses.	
	Vigência:	12 meses (2024)	
	Modalidade do Serviço:	*On-premise* (licença perpétua)	
	Tipo da Contratação:	**Inexigibilidade de Licitação**	
	Arquivo:	[7] CCOMGEX - Contrato 07-2023 - Plataforma GRC Modulo.pdf	
	Item	**Descrição do Item**	**Valor Unitário**
	1	Contratação do Suporte, Manutenção e Atualização de Licença do Software de Governança. Risco e Conformidade (GRC) Risk Manager, com Garantia Técnica, pelo período de 12 (doze) meses.	R$ 230.749,20
		Valor Total do Contrato	R$ 230.749,20
		Valor Anual	**R$ 230.749,20**

Contrato 3			
	Órgão / Instituição:	Companhia Riograndense de Saneamento - CORSAN	
	Instrumento Contratual:	Contrato nº 153/2022	
	Contratada:	Modulo Security Solutions	
	Objeto:	RENOVAÇÃO DO SOFTWARE MÓDULO RISK MANAGER COM MÓDULOS DE ATENDIMENTO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD), CONTEMPLANDO O FORNECIMENTO DE SUPORTE TÉCNICO PARA IMPLANTAÇÃO, PARAMETRIZAÇÃO E CAPACITAÇÃO,	
	Vigência:	12 meses (2022)	
	Modalidade do Serviço:	*On-premise* (licença perpétua)	
	Tipo da Contratação:	**Inexigibilidade de Licitação**	
	Arquivo:	Corsan.pdf	
	Item	**Descrição do Item**	**Valor Unitário**
	1	RENOVAÇÃO DO SOFTWARE MÓDULO RISK MANAGER	R$239.500,00
		Valor Total do Contrato	R$239.500,00
		Valor Anual	**R$239.500,00**

1.3.2 Outras soluções disponíveis

Em matéria de softwares, apenas soluções de GRC ou estritamente de Análises de Riscos poderiam fornecer ferramentas para o trabalho adequado na área de Gestão de Riscos de Segurança da Informação e Riscos Cibernéticos. Portanto, a aquisição de um software de GRC está alinhado com a necessidade.

Não considerando a aquisição de softwares, a Gestão de Riscos de Segurança deveria ser desempenhada única e exclusivamente sem apoio de sistemas especificamente desenvolvidos para isso, dependendo de mão de obra em quantia necessária para o planilhamento de dezenas, eventualmente, centenas de ativos da organização que devem ter os riscos mapeados. Considerando os recursos humanos hoje existentes, e o fato que a metodologia de análise de riscos seria definitivamente afetada, a não aquisição de uma solução não é considerada uma opção válida para atendimento da necessidade ora pontuada.

1.3.3 Alternativa no mercado de TI

Não há alternativa, tratando-se de software livre ou público, que seja aderente aos requisitos listados pelo TRT9. Pontua-se que o uso software livre ou público demanda de instalação, configuração, parametrização e manutenção constante, onerando a equipe interna que deveria estar justamente apenas operando e utilizando os recursos da solução. Como um dos objetivos é migrar dados para nuvem e desfrutar da utilização de infraestrutura da fabricante, não se vê como oportuno, neste momento, manter uma infraestrutura que suporta a solução GRC, seja ela qual for, localmente, dentro da rede corporativa do Tribunal, demandando de constante manutenção e atenção às vulnerabilidades da solução.

1.3.4 Análise comparativa de soluções

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução Única	X		
A Solução está disponível no Portal do Software Público Brasileiro?	Solução Única		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução Única		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução Única			X
A Solução é aderente às regulamentações da ICP-Brasil?	Solução Única			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução Única			X
A Solução observa as orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus).	Solução Única			X
A Solução observa as políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário.	Solução Única			X

1.3.5 Mapa comparativo de preços / Análise dos custos totais da demanda

Analisando-se os valores das contratações públicas similares encontradas e o valor da proposta comercial recebida, nota-se que a proposta possui valores mais baixos, para escopos bem parecidos.

ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DA DEMANDA				
	Órgão	**Objeto**	**Valor Total**	**Valor por Um Ano**
1	ANVISA	Contratação de serviços de Suporte Técnico ao Software Módulo Risk Manager com atualização de versão, tendo como objetivo manter a solução sempre atualizada e em pleno funcionamento (**Primeiro Termo Aditivo**).	R$ 880.000,00	R$ 440.000,00
2	CCOMGEX	Contratação do Suporte, Manutenção e Atualização de Licença do Software de Governança. Risco e Conformidade (GRC) Risk Manager, com Garantia Técnica, pelo período de 12 (doze) meses.	R$ 230.749,20	R$ 230.749,20
3	CORSAN	Contratação do Suporte, Manutenção e Atualização de Licença do Software de Governança. Risco e Conformidade (GRC) Risk Manager, com Garantia Técnica, pelo período de 12 (doze) meses.	R$239.500,00	R$239.500,0

O mapa comparativo de preços consta do anexo **Mapa Comparativo de Preços - IN 73-2020 - Risk Manager.pdf**

1.3.6 Detalhamento e justificativa da solução escolhida

Nome da Solução: Contratação do módulo Cybersecurity Manager da plataforma Risk Manager, incluindo a migração de dados da licença perpétua do Risk Manager para nuvem (SaaS – software como serviço), treinamento e suporte técnico por 12 (doze) meses fornecida pela empresa Modulo Security Solutions S/A.	
Justificativa	Única solução que atende aos requisitos listados pelo TRT9, de acordo com a pesquisa de mercado.
Benefícios	● Fornecer continuidade e melhoria nos processos de gestão de riscos de Segurança da Informação, Segurança Cibernética e de riscos de Tecnologia da Informação e Comunicação; ● Suportar ações relacionadas ao processo de Continuidade de Serviços Essenciais de TIC e na confecção do Plano de Continuidade; ● Apoiar a implantação de controles de Segurança da Cibernética e conformidade com frameworks e normas comuns ao mercado; ● Buscar a conformidade com recomendações, resoluções e normas dos órgãos de controle para a área de segurança de TI; ● Auxiliar na priorização de investimentos para redução de custos em contratações na área de segurança de TIC; ● Manter a automatização do processo de trabalho de análise de riscos de segurança; ● Fornecer uma visão gerencial dos riscos, com indicadores e métricas definidas.
Locais de utilização do serviço	Secretaria Geral de Tecnologia da Informação e Comunicação – SGTIC

Cronograma

ITEM	DESCRIÇÃO DO ITEM	PRAZO
1	SaaS - Plataforma Risk Manager para nuvem.	Disponibilidade no acesso em até 10 dias após a assinatura do contrato.
2	SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem.	Disponibilidade no acesso em até 10 dias após a assinatura do contrato.
3	Migração de dados da licença perpétua do Risk Manager para nuvem.	Finalização da migração em até 30 dias após a assinatura do contrato.
4	Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.	Execução do treinamento em até 60 dias após a assinatura do contrato.
5	Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.	Término do serviço em até 90 dias após a assinatura do contrato.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, V: "*V - levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar;*" c/c Res. CSJT 364/2023, art. 33, V: "V - *levantamento de mercado com análise das alternativas de soluções e justificativa técnica e econômica da escolha e do tipo de solução a contratar.*".

1.4 Descrição da solução como um todo

Contratação de plataforma de solução GRC (Governança, Riscos e Conformidade) em nuvem da mesma fabricante do software Modulo Risk Manager com licenças perpétuas já instalado no TRT9, porém sem suporte nem garantia de atualização, com migração dos dados hoje salvos localmente para base de dados em nuvem e aquisição de expansão da plataforma, focada em gestão de riscos de segurança cibernética e treinamento para o novo módulo e para plataforma principal, visando aprimorar, primeiramente, a gestão de riscos de segurança da informação e segurança cibernética no Tribunal.

1.5 Estimativa das quantidades a serem contratadas

ITEM	DESCRIÇÃO DO ITEM	QTD	JUSTIFICATIVA
1	SaaS - Plataforma Risk Manager para nuvem.	1	Subscrição de serviço com pagamento mensal em 12 parcelas. O acesso será concedido para até 20 usuários concorrentes, sem nominação das licenças.
2	SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem.	1	Subscrição de serviço com pagamento mensal em 12 parcelas. O acesso será concedido para até 20 usuários concorrentes, sem nominação das licenças.
3	Migração de dados da licença perpétua do Risk Manager para nuvem.	1	Serviço necessário para migração de dados da infraestrutura e base de dados locais para nuvem.
4	Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.	1	Visando expandir a operação, o treinamento da operação da plataforma principal e do novo módulo será fornecido para mais pessoas associadas aos trabalhos de gestão de riscos da SGTIC.

5	Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.	1	Horas técnicas calculadas com base em um expediente interno diário de 7 horas, durante 20 dias úteis de trabalho em conjunto entre as equipes do TRT9 e da Modulo.

1.5. 1 Demanda prevista por quantidade de bens e serviços

ID	Item demandado	Demanda Prevista	Quantitativo a ser contratado	Critérios de medição utilizados, documentos e outros meios probatórios
1	SaaS - Plataforma Risk Manager para nuvem.	1	1	Não é possível a contratação de acesso menor que uma unidade.
2	SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem.	1	1	Não é possível a contratação de acesso menor que uma unidade.
3	Migração de dados da licença perpétua do Risk Manager para nuvem.	1	1	Não é possível a contratação do serviço de migração de dados menor que uma unidade.
4	Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.	1	1	Unidades que poderão ser beneficiadas com o treinamento: SGSI – 3 pessoas CGSI – 1 pessoa CSGTI – 2 pessoas SGSTIC (Unidades de apoio e Governança) – 4 pessoas
5	Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.	1	1	Horas técnicas calculadas com base em um expediente interno diário de 7 horas, durante 20 dias úteis de trabalho em conjunto entre as equipes do TRT9 e da Modulo. Não é possível contratar serviço de migração de dados menor que uma unidade.

Fundamentação: Lei n. 14.133/2021, art. 18, § 1º, IV: "*IV - estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala;*" c/c Res. CSJT 364/2023, art. 33, IV.

1.6 Estimativa do valor da contratação

O valor estimado da contratação é de **R$ 126.400,00**, sendo R$ 53.200,00 para pagamento em parcelas únicas, pela prestação de serviços pontuais (migração de dados, treinamento e operação assistida) e R$ 73.200,00 pagos em parcelas mensais, relativas à subscrição do acesso às plataformas em nuvem da solução.

Fundamentação: Lei n. 14.133/2021, art. 18, § 1º, VI: "VI - estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação;" c/c Res. CSJT 364/2023, art. 33, VI.

1.7 Justificativa para o parcelamento ou não da solução

Os serviços contratados são de fornecimento exclusivo da Modulo Security Solutions S/A, conforme critérios de atendimento estabelecidos pela fabricante e não podem ser parcelados.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, VIII: "VIII - justificativas para o parcelamento ou não da contratação;" c/c Res. CSJT 364/2023, art. 33, VIII: "VIII - justificativas para o parcelamento ou não do objeto, quando necessário para sua individualização.;".

1.8 Contratações correlatas e/ou interdependentes

Não há contratações correlatas ou interdependentes a serem executadas nessa contratação.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, XI: "XI – contratações correlatas e/ou interdependentes;" c/c art. 33 XI da Res. CSJT 364/2023.

1.9 Demonstrativo da previsão da contratação no Plano de Contratações Anual, Orçamento Estimado e Alinhamento Estratégico

A necessidade foi incluída no Plano Anual de Contratações de 2024, aprovado por meio do Despacho ADG 43 PROAD 4971-23.

Item PLOA : 151102024338547

Descrição no Plano de Contratações: GOVERNANÇA - Solução de Gerenciamento de Riscos (Suporte) - Risk Manager - PO-TI - CSIR

Item Execução Orçamentária: 151102024000157

Alinhamento Estratégico:

PEI: OE03 - Aprimorar a Governança de TIC, a proteção de dados e a segurança cibernética

ENTIC-JUD: OE 7 - Aprimorar a Segurança da Informação e a Gestão de Dados

Fundamentação: Lei 14.133/2021, art. 18, § 1º, II: "*II - demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração;*" c/c art. 33 da Res. CSJT 364/2023, II: "*II – o alinhamento planejamento estratégico institucional, ao plano de logística sustentável e à previsão no Plano de Contratação Anual, observando os temas e indicadores definidos nos referidos instrumentos;*".

1.10 Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais ou financeiros disponíveis:

Com a migração da base de dados local da plataforma Risk Manager para versão em nuvem disponibilizada e mantida pelo fabricante, espera-se uma melhor eficiência no uso da ferramenta, pois não haverá mais a necessidade de manter uma 'máquina virtual' e toda infraestrutura associada para que o sistema opere localmente. O uso da plataforma em nuvem facilitará em muito a manutenção da solução, pois a responsabilidade de atualização do software ficará a cargo da fabricante, permitindo economia de tempo na manutenção da plataforma e direcionando esse tempo para operação da solução, que é o foco da contratação em si. Além do mais, a expansão Cybersecurity Manager não funciona, nativamente, em ambiente local (on premise), sendo desenvolvida para acesso e operação em nuvem.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, IX: "IX - demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;", c/c art. 33 da Res. CSJT 364/2023, IX.

1.11 Providências para adequação do ambiente do órgão (Relacionar os ajustes e adequações que precisam ser realizados no ambiente do órgão para viabilizar a implantação e a sustentação da STIC escolhida).

AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL		
Nome da Solução Única:	Contratação do módulo Cybersecurity Manager da plataforma Risk Manager, incluindo a migração de dados da licença perpétua do Risk Manager para nuvem (SaaS – software como serviço), treinamento e suporte técnico por 12 (doze) meses.	
ID	Tipo de necessidade	Descrição
1	Infraestrutura tecnológica	Sem necessidade de alterações.
2	Infraestrutura elétrica	Sem necessidade de alterações.
3	Logística de implantação	Sem necessidade de alterações.
4	Espaço físico	Sem necessidade de alterações.
5	Mobiliário	Sem necessidade de alterações.
7	Necessidade de capacitação	Necessário conforme requisitos descritos neste estudo.

Fundamentação: Lei 14.144/2021, art. 18, § 1º, X: "X - providências a serem adotadas pela Administração previamente à celebração do contrato, inclusive quanto à capacitação de servidores ou de empregados para fiscalização e gestão contratual;" c/c art. 33 da Res. CSJT 364/2023, X: "X - providências para adequação do ambiente do órgão, se necessário, bem como quanto à capacitação de servidores para fiscalização e gestão contratual;".

1.12. Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras:

Não se vislumbra possíveis impactos ambientais resultantes desta contratação.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, XII: "XII - descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável;" c/c art. 33 da Res. CSJT 364/2023, XII.

1.13. Posicionamento conclusivo sobre a adequação da contratação à necessidade a que se destina:

Conclui-se que o conjunto de requisitos descritos neste estudo e o objeto desta contratação estão alinhados à necessidade da organização.

Fundamentação: Lei 14.133/2021, art. 18, § 1º, XIII: "XIII - posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina", c/c art. 33 da Res. CSJT 364/2023, XIII.

1.14 Análise da necessidade de classificação nos termos da Lei n° 12.527, de 18 de novembro de 2011

Nenhum documento produzido pela equipe de planejamento (ETP, TR, pesquisa de preços, etc.) terá caráter sigiloso.

Fundamentação: Lei n. 14.133/2021, art. 6º, XXIII, "b", c/c IN SEGES 58/2022, art. 13: "Art. 13. Ao final da elaboração do ETP, deve-se avaliar a necessidade de classificá-lo nos termos da Lei nº 12.527, de 18 de novembro de 2011.".

1.15 Análise do processamento por meio do sistema de registro de preços.

Não se aplica

Fundamentação: Lei n. 14.133/2021, art. 40 (O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte.); Decreto nº 11.462/2023, art. 3º (O SRP poderá ser adotado quando a Administração julgar pertinente, em especial: I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes; II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa; III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas; IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.).

2 SUSTENTAÇÃO DO CONTRATO

2.1 Recursos materiais e humanos

Haverá a necessidade de envolvimento da equipe do TRT9 principalmente para o trabalho colaborativo de parametrização do uso do novo módulo contratado, de acordo com as necessidades do Tribunal, e para o auxílio à equipe da CONTRATADA por ocasião da migração dos dados da plataforma local para nuvem.

A quantidade de recursos humanos é variável e depende de ações específicas necessárias e que agora não podem ser previstas, em virtude das características da rede corporativa e dos requisitos técnicos para execução do serviço pela CONTRATADA.

Não haverá necessidade de emprego de recursos materiais para esse processo.

2.2 Gestão e fiscalização contratual

A gestão e a fiscalização dos contratos administrativos serão realizadas conforme disposto no Ato Presidência nº 164, de 06 de junho de 2023, combinado com a Resolução CNJ 468/2022.

2.3 Descontinuidade do fornecimento da solução de tecnologia da informação

- Os acessos às plataformas SaaS serão encerrados de forma automática ao final do contrato;
- Em caso de rescisão ou encerramento do contrato da licença SaaS, todos os dados do CONTRATANTE serão armazenados na nuvem da CONTRATADA por até 60 (sessenta) dias, a contar da data de finalização do contrato, com disponibilidade para retirada dos dados por parte do CONTRATANTE;
    - No caso de finalização contratual sem prorrogação, os dados, sob a guarda da CONTRATADA, devem ser requisitados pelos canais de suporte dentro do prazo de 60 (sessenta) dias após o fim do contrato;
    - Após esse período, os dados serão destruídos por parte da CONTRATADA;
- Este contrato não contempla o serviço de migração da infraestrutura em nuvem da CONTRATADA para infraestrutura local do CONTRATANTE;
    - Caso haja interesse do TRT9 migrar os dados em nuvem para o Risk Manager instalado na infraestrutura do Tribunal, será necessária uma o estabelecimento de instrumento contratual específico para esse fim, com base em cotação comercial para o serviço de migração dos dados em nuvem para on premise, em até 60 (sessenta) dias após encerramento do contrato.

2.4 Transição contratual

ID	Ação	Responsável	Data Início	Data Fim
1	Solicitação, mediante chamado técnico, à CONTRATADA dos dados do Tribunal salvos em nuvem.	Fiscal do Contrato	No máximo na data final do contrato	Até 30 (trinta) dias após finalização contratual
2	Importação dos dados para o ambiente on premise, com licenças perpétuas, do software Risk Manager	Operador local da solução	Após finalização contratual	---

2.5 Estratégia de independência tecnológica

Em caso de rescisão ou encerramento do contrato da licença SaaS, todos os dados do CONTRATANTE serão armazenados na nuvem da CONTRATADA por até 60 (sessenta) dias, a contar da data de finalização do contrato, com disponibilidade para retirada dos dados por parte do CONTRATANTE:

- No caso de finalização contratual sem prorrogação, os dados, sob a guarda da CONTRATADA, devem ser requisitados pelos canais de suporte dentro do prazo de 60 (sessenta) dias após o fim do contrato;
- Após esse período, os dados serão destruídos por parte da CONTRATADA.

Não se trata de contratação de desenvolvimento de softwares, sejam estratégicos ou não, e nem é possível considerar a migração para plataforma software livre dos dados gerados pelo TRT9 e salvos em nuvem.

Fundamentação: Resolução CNJ 370/ 2021, art.32. Na contratação de desenvolvimento de sistemas de informação considerados estratégicos, em que a propriedade intelectual não é da pessoa de direito público contratante, o órgão deverá fazer constar no instrumento contratual cláusula que determine o depósito da documentação e afins pertinentes à tecnologia de concepção, manutenção e atualização, bem como, quando cabível, do código fonte junto a autoridade brasileira que controla a propriedade intelectual de softwares para garantia da continuidade

3 ESTRATÉGIA PARA A CONTRATAÇÃO

3.1 Natureza do objeto

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

A prestação do serviço de acesso à SaaS pode se estender por mais de um exercício financeiro.

DETALHAMENTO DOS BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO	
ID	**SERVIÇOS QUE COMPÕEM A SOLUÇÃO**
1	SaaS - Plataforma Risk Manager para nuvem.
2	SaaS – Módulo Cybersecurity Manager da Plataforma Risk Manager para nuvem.
3	Migração de dados da licença perpétua do Risk Manager para nuvem.
4	Treinamento remoto do módulo Cybersecurity Manager e da Plataforma Risk Manager em turma de até 10 pessoas.
5	Operação Assistida para implantação do módulo Cybersecurity Manager da expansão do Risk Manager por 140 horas.

3.2 Adjudicação do objeto

Adjudicação global. A fabricante Modulo Security Solutions S/A é a única empresa que pode executar os serviços de software para a plataforma Risk Manager, visto ser a fabricante da solução.

3.3 Modalidade e tipo de licitação

A seleção do fornecedor dar-se-á por **Inexigibilidade de Licitação**, visto que a fabricante Modulo Security Solutions S/A detém atestado de exclusividade de prestação especializada de serviços de suporte e garantia para a plataforma Risk Manager, conforme **Certificado de Propriedade**, emitido pela **Fenainfo**, conforme arquivo '[8] Modulo - Certificado de Propriedade - Exclusividade - FENAINFO.pdf'

3.3.1 Análise do processamento por meio do sistema de registro de preços

Não aplicável, pois se trata de processo de aquisição via inexigibilidade de licitação.

Fundamentação: Lei n. 14.133/2021, art. 40 (O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte.); Decreto nº 11.462/2023, art. 3º (O SRP poderá ser adotado quando a Administração julgar pertinente, em especial: I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes; II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa; III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas; IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.)

3.4 Classificação e indicação orçamentária

CLASSIFICAÇÃO ORÇAMENTÁRIA – FONTE DE RECURSOS		
ID	**Valor**	**Fonte (Programa / Ação)**
1	R$ 43.200,00	2141713 / 0100000000 / 3.3.90.40
2	R$ 30.000,00	2141713 / 0100000000 / 3.3.90.40
3	R$ 18.000,00	2141713 / 0100000000 / 3.3.90.40
4	R$ 10.000,00	2141713 / 0100000000 / 3.3.90.40
5	R$ 25.200,00	2141713 / 0100000000 / 3.3.90.40
TOTAL	**R$ 126.400,00**	

3.5 Vigência da prestação de serviço

A vigência prevista é de 12 (doze) meses, contados a partir da assinatura do contrato.

3.6 Equipe de apoio à contratação

Informar, nos termos do Ato Presidência nº 164/2023, a equipe responsável pela gestão e fiscalização contratual.

Gestor do Contrato:	Alexandre Tetsuo Yamauchi / Secretaria de Infraestrutura e Operações
Fiscal Técnico Titular:	Robson Cleiton Novak / Núcleo de Gestão da Segurança da Informação
Fiscal Técnico Substituto:	Oeslei Taborda Ribas / Seção de Operação da Segurança da Informação
Fiscal Administrativo:	Paulo Celso Gerva / Secretaria de Licitações e Contratos

3.7 Recebimento

A equipe de recebimento instituída assinará apenas o primeiro termo de recebimento de serviço, conforme modelo local do sistema interno de tramitação processual (PROAD), por ocasião do recebimento da primeira nota fiscal referente ao pagamento dos itens 1 e 2 (serviço continuado), e assinará os termos de recebimentos no sistema para os serviços descritos nos itens 3, 4 e 5 por ocasião do recebimento das respectivas notas fiscais após realização dos serviços prestados de acordo com os prazos definidos nos requisitos temporais deste estudo.

Fundamentação: Res. CNJ 468/2022, art. 22 – "A equipe de gestão de contrato é composta pelo gestor do contrato, responsável por gerir a execução contratual e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual. " ...

"§ 2o O papel de gestor do contrato não pode ser acumulado com nenhum outro papel da equipe de gestão da contratação. "

Res. CNJ 468/2022, art. 24: "O gestor do contrato, os fiscais demandantes, técnico e administrativo do contrato, poderão ser os mesmos servidores que realizaram o planejamento da contratação, desde que atendam os princípios da vantajosidade e economicidade para a administração pública"...

"§ 1º Os papéis de fiscais não poderão ser acumulados pelo mesmo servidor, salvo quanto aos papéis de fiscal demandante e técnico, em casos excepcionais, mediante justificativa fundamentada nos autos e aprovado pelo superior imediato do dirigente da área de TI".

"§ 3o O fiscal administrativo deverá ser designado pela autoridade competente e não poderá ser servidor da área de TIC, salvo em situações excepcionais, devidamente justificada."

4 ANÁLISE DE RISCOS – MAPA DE RISCOS (DOCUMENTO EM ANEXO)

4.1 Riscos do processo de contratação e da solução de TI

- Não realizar ampla pesquisa de mercado na fase de elaboração do ETP;
- Especificação incompleta ou incorreta da solução desejada;
- Não aderência da solução aos requisitos especificados;
- Contingenciamento orçamentário interno à organização ou redirecionamento do recurso reservado para outro fim.

4.2 Riscos relacionados ao não atendimento das necessidades do TRT9 pelos serviços prestados pela contratada

4.2.1 Riscos de negócio

- Falta de capacitação dos profissionais da contratada;
- Falha no atendimento aos chamados nos prazos;
- Falta de recursos (de pessoal, financeiro e tecnológico);
- Não cumprimento do Acordo de Nível de Serviço.

4.2.2 Riscos tecnológicos

- Funcionalidades previstas não funcionarem conforme inicialmente previsto;
- Necessidade de alterar níveis de segurança tecnológica para a integração da ferramenta funcionar adequadamente.

4.2.3 Riscos de pessoal

- Dificuldades dos administradores na operação do ambiente;
- Falta de pessoal para efetuar a administração do sistema;
- Saída de membros da equipe;
- Falhas na execução das cláusulas contratuais;
- Falta de treinamento ou treinamento insuficiente para lidar com as peculiaridades do equipamento.

4.2.4 Riscos externos

- Contingenciamento orçamentário por conta da política econômica federal que afete o planejamento de despesas do projeto;
- Não continuidade desenvolvimento da solução no mercado, deixando de fornecer atualizações à plataforma;
- Alterações no panorama econômico da CONTRATADA durante a apresentação da proposta e a assinatura do contrato.

Mapa de Riscos (elemento obrigatório)

Fundamentação: Lei n. 14.133/2021, art. 18, X: "X a análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual;", c/c art. 51 da Res. CSJT 364/2023, § 2º.

<table>
<tr><th>ITENS ADICIONAIS</th><th>DESCRIÇÃO</th></tr>
<tr><td>A</td><td>Lista de Potenciais Fornecedores

Nome: Modulo Security Solutions S/A
CNJP: 28.712.123/0001-74
Sítio da Internet: https://www.modulo.com.br/
Contato: Alexandre Lyra – Gerente Comercial
E-mail: alyra@modulo.com
Telefones: (21) 99111-3120 (WhatsApp)
96606-2073 (Telegram)</td></tr>
<tr><td>B</td><td>Contratações Públicas Similares

<table>
<tr><th>Órgão / Instituição</th><th>Contrato</th><th>Objeto</th></tr>
<tr><td>ANVISA</td><td>14/2020</td><td>Contratação de serviços de Suporte Técnico ao Software Módulo Risk Manager com atualização de versão, tendo como objetivo manter a solução sempre atualizada e em pleno funcionamento.</td></tr>
<tr><td>CCOMGEX</td><td>07/2023</td><td>Contratação do Suporte, Manutenção e Atualização de Licença do Software de Governança. Risco e Conformidade (GRC) Risk Manager, com Garantia Técnica, pelo período de 12 (doze) meses.</td></tr>
<tr><td>CORSAN</td><td>153/2022</td><td>Contratação de serviços de Suporte Técnico ao Software Módulo Risk Manager com atualização de versão, pelo período de 12 (doze) meses</td></tr>
</table>
</td></tr>
<tr><td>C</td><td>Memórias de Cálculos
Mapa Comparativo de Preços - IN 73-2020 - Risk Manager.pdf</td></tr>
<tr><td>D</td><td>Mapa de Riscos (documento em anexo)
Mapa de Riscos - Risk Manager.pdf</td></tr>
</table>

Equipe de Planejamento da contratação:

Paulo Roberto Nunes

Integrante Demandante

Robson Cleiton Novak

Integrante Técnico

Paulo Celso Gerva

Integrante Administrativo