

ESTUDOS PRELIMINARES

I – ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 ESPECIFICAÇÃO DOS REQUISITOS

1.1 DE NEGÓCIO

1.1.1 A solução deverá:

1.1.1.1 Permitir a educação e conscientização em segurança da informação, com simulação de *phishing*.

1.1.1.1.1 Acesso ilimitado à biblioteca com, no mínimo, 300 (trezentos) itens de conteúdo de segurança da informação em português ou em língua estrangeira com legendas em português.

1.1.1.1.2 Entregar conhecimento através de conteúdos, tais como: vídeos, *games*, *quizzes*, artes (*posteres*), *assessments* (avaliações).

1.1.1.1.3 Permitir inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários.

1.1.1.1.4 Permitir a carga de conteúdos próprios de treinamento em segurança da Informação da contratante, em vídeo, no formato *PDF* ou no padrão *SCORM*.

1.1.1.1.5 Permitir a carga e o aceite de políticas e normas de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte.

1.1.1.1.6 Prover ambiente de gestão para acompanhamento online de progressão e desempenho dos usuários.

1.1.1.1.7 Disponibilizar detalhes sobre a porcentagem de inscrições, cursos iniciados, incompletos, concluídos e conhecimento da política de segurança e normas.

1.1.1.1.8 Prover ambiente de gestão que possibilite a criação de grupos de usuários com base em comportamento frente as simulações e treinamentos realizados.

1.1.1.1.9 Disponibilizar relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos.

1.1.1.1.10 Permitir a emissão de certificados para os treinamentos.

1.1.1.1.11 Prover *APIs* de relatórios que permitam personalizar os documentos, integrando-os a outros sistemas de negócios para apresentar os dados a partir da plataforma.

1.1.1.1.12 Disponibilizar perfis de acesso para gestão de campanhas e treinamentos (desejável também perfil para auditoria, porém não obrigatório).

1.1.1.1.13 Possibilitar a autenticação em dois fatores para usuários e administradores.

1.1.1.1.14 Possibilitar a criação de campanhas simuladas de *phishing*, a fim de avaliar o comportamento dos usuários.

1.1.1.1.15 Prover gerenciamento de usuários e cursos, permitindo.

1.1.1.1.16 Possibilitar a criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco

em segurança da informação dos usuários.

1.1.1.1.17 Apresentar painel gerencial com indicador de nível de risco em segurança da informação para cada usuário e para a instituição.

1.1.1.1.18 Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br).

1.1.1.1.19 Prover APIs que permitam a exportação contínua de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante.

1.1.2 Atualmente existe a necessidade de aquisição de plataforma de educação e conscientização em segurança da informação, conforme abaixo:

| Item | Descrição | Tipo |
|------|--|---|
| 1 | Licenciamento de plataforma de educação e conscientização em segurança da informação | |
| 2 | Serviço de instalação e configuração da solução | - |
| 3 | Repasso tecnológico | Por um período mínimo de 20 (vinte) horas |
| 4 | Suporte técnico | Durante o período contratual |

1.2 DE CAPACITAÇÃO

1.2.1 Haverá necessidade de treinamento ou repasse tecnológico, presencial ou a distância, visando capacitar os servidores da Secretaria de Tecnologia da Informação e Eleições (STIE) no uso da ferramenta.

1.2.2 Deverá haver uma instrução no modelo *hands-on* para gestores da plataforma.

1.3 LEGAIS

1.3.1 A contratação obedecerá às regras gerais de fornecimento ao Poder Público, inexistindo requisitos legais específicos para essa contratação.

1.4 MANUTENÇÃO

1.4.1 Suporte técnico deverá estar disponível durante a vigência de uso da licença.

1.4.2 Atualizações da solução deverão estar disponíveis durante a vigência de uso da licença.

1.5 TEMPORAIS

1.5.1 A fornecedora da solução terá até **05 (cinco) dias** contados após a formalização da contratação para fornecer os softwares ou as subscrições contratadas.

1.6 DE SEGURANÇA

- 1.6.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL, em especial:
- 1.6.1.1 O fornecedor assinará, no ato da entrega das licenças e do serviço, 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.
- 1.6.1.2 Da gestão de ativos.
- 1.6.1.3 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da JUSTIÇA ELEITORAL ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação devendo orientar seus funcionários nesse sentido.
- 1.6.1.4 Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pela JUSTIÇA ELEITORAL, durante o tempo de permanência nas suas dependências, observando a Portaria 226/2018-GP-TRE/RN, que dispõe sobre as medidas de controle de acesso, circulação e permanência de pessoas nos prédios do Edifício-Sede do Tribunal Regional Eleitoral do Rio Grande do Norte, do Centro de Operações da Justiça Eleitoral (COJE), Fórum Eleitoral de Natal e, no que couber, aos prédios das Zonas Eleitorais do Interior do Estado.

1.7 SOCIAIS, AMBIENTAIS E CULTURAIS

- 1.7.1 É de responsabilidade da empresa fornecedora da solução a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos.
- 1.7.2 O Tribunal Regional Eleitoral do Rio Grande do Norte reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração.
- 1.7.3 Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclagem efetiva no Brasil.
- 1.7.4 Deverá possuir conteúdo acessível à deficientes auditivos e visuais.
- 1.7.5 Deverá permitir a inclusão da identidade visual da instituição nas campanhas e treinamentos.
- 1.7.6 O ambiente da plataforma deverá ser disponibilizado totalmente em português.

1.8 DE ARQUITETURA TECNOLÓGICA

1.8.1 A fim de tornar-se um dos pilares para a execução de um programa permanente de conscientização em segurança da informação na Justiça Eleitoral, a solução deve prover, no mínimo os seguintes recursos:

1.8.1.1 Acesso ilimitado à biblioteca com, no mínimo, 300 (trezentos) itens de conteúdo de segurança da informação em português ou em língua estrangeira com legendas em português. Requisitos adicionais:

1.8.1.1.1 A plataforma deve estar em conformidade com o padrão WCAG (versão 2 ou superior), para atender as necessidades de usuários com deficiências visuais, auditivas, motoras e cognitivas.

1.8.1.1.2 Deve haver na plataforma conteúdo específico voltado a LGPD Brasileira.

1.8.1.2 A solução deverá entregar conhecimento através de conteúdos, tais como: vídeos, *games*, *quizzes*, artes (*posteres*), assessments (avaliações).

1.8.1.3 A solução deverá prover gerenciamento de usuários e cursos, permitindo:

1.8.1.3.1 Seleção de módulos de treinamento para grupo de usuários.

1.8.1.3.2 Atribuição automática de treinamentos para novos usuários.

1.8.1.3.3 Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes.

1.8.1.3.4 Carga de usuários por meio de arquivo .CSV.

1.8.1.3.5 Integração com o AD (*Active Directory*) da contratante.

1.8.1.3.6 Inativação de usuários sem perda do histórico de dados.

1.8.1.3.7 Permitir que uma licença de acesso utilizada por um usuário desligado da contratante possa ser aplicada a um novo usuário, durante o período remanescente da contratação.

1.8.1.3.7.1 Neste caso, não é necessária a manutenção do histórico do usuário antigo.

1.8.1.4 A solução deverá permitir inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários.

1.8.1.5 A solução deverá permitir a carga de conteúdos próprios de treinamento em segurança da Informação da contratante, em vídeo, no formato PDF ou no padrão SCORM.

1.8.1.5.1 Todas as funcionalidades da gestão disponíveis para os conteúdos nativos devem poder ser aplicadas aos conteúdos próprios da contratante.

1.8.1.6 A solução deverá permitir a carga e o aceite de políticas e normas de segurança da informação da contratante.

1.8.1.7 A solução deverá prover ambiente de gestão para acompanhamento *online* de progressão e desempenho dos usuários.

1.8.1.8 A solução deverá disponibilizar detalhes sobre a porcentagem de inscrições, cursos iniciados, incompletos, concluídos e conhecimento da política de segurança e normas.

1.8.1.9 A solução deverá prover ambiente de gestão que possibilite a criação de grupos de usuários com base em comportamento frente as simulações e treinamentos realizados.

1.8.1.10 A solução deverá disponibilizar relatórios executivos e de gestão sobre as campanhas e resultados

de treinamentos.

1.8.1.11 A solução deverá permitir a emissão de certificados para os treinamentos.

1.8.1.12 A solução deverá prover *APIs* de relatórios que permitam personalizar os documentos, integrando-os a outros sistemas de negócios para apresentar os dados a partir da plataforma.

1.8.1.13 A solução deverá disponibilizar perfis de acesso para gestão de campanhas e treinamentos (desejável também perfil para auditoria, porém não obrigatório).

1.8.1.14 A solução deverá possibilitar a autenticação em dois fatores para usuários e administradores.

1.8.1.15 A solução deverá possibilitar a criação de campanhas simuladas de *phishing*, a fim de avaliar o comportamento dos usuários:

1.8.1.15.1 Permitir criação de número ilimitado de campanhas durante a vigência da contratação.

1.8.1.15.2 Disponibilizar pelo menos 50 (cinquenta) modelos de campanhas em português e permitir a personalização dos modelos diretamente pela contratante.

1.8.1.15.3 Manter histórico por usuário e por campanha.

1.8.1.15.4 Permitir que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação.

1.8.1.16 A solução deverá possibilitar a criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários.

1.8.1.17 A solução deverá apresentar painel gerencial com indicador de nível de risco em segurança da informação para cada usuário e para a instituição.

1.8.1.17.1 O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de *phishing*.

1.8.1.18 A solução deverá disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br).

1.8.1.19 Para evitar dependência tecnológica, a plataforma deve prover *APIs* que permitam a exportação contínua de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante.

1.8.1.19.1 Informações como evolução da maturidade dos usuários (nível de risco), cursos efetuados, certificados, resultados de testes de *phishing*, etc, devem ser passíveis de exportação através de *APIs*.

1.8.1.19.2 Essa característica permite que a Justiça Eleitoral, ao término da contratação, possa prosseguir com seu programa contínuo de capacitação, na forma determinada pelo TCU no Acórdão Plenário 3143/2021.

1.9 DE PROJETO E DE IMPLEMENTAÇÃO

1.9.1 Não se aplica.

1.10 DE IMPLANTAÇÃO

1.10.1 O serviço de implantação poderá ser executado presencialmente na Sede do Tribunal Regional Eleitoral do Rio Grande do Norte ou remotamente, acompanhados e supervisionados por sua equipe técnica e realizados prioritariamente durante o expediente normal da Justiça Eleitoral do Rio Grande do Norte.

1.10.1.1 Caso necessário, visando minimizar o impacto para os usuários, o Tribunal Regional Eleitoral do Rio Grande do Norte poderá exigir a execução da implantação fora do horário de expediente normal, ou seja, durante a noite, a madrugada ou em finais de semana e feriado.

1.10.1.2 A fornecedora da solução deverá disponibilizar, durante todo período contratual, um Gerente de Contas para apoiar e orientar o Tribunal Regional Eleitoral do Rio Grande do Norte no uso da plataforma.

1.10.1.2.1 As atividades do gerente de contas podem ser desenvolvidas remotamente, com uso de meios de comunicação digital.

1.10.1.2.2 O gerente de conta tem como atribuições:

1.10.1.2.3 Acompanhar o projeto (programa de conscientização).

1.10.1.2.4 Esclarecer dúvidas.

1.10.1.2.5 Sugerir proativamente novos caminhos para o programa.

1.10.1.2.6 Ser ponte com o suporte técnico.

1.10.1.2.7 Configurar a conta e fazer a integração com a infraestrutura da contratante (*onboarding*).

1.10.2 A fornecedora da solução deverá efetuar, a partir das informações fornecidas pelo Tribunal Regional Eleitoral do Rio Grande do Norte, a implantação da solução (*onboarding*), tarefa que consiste na configuração e integração da infraestrutura tecnológica da contratante com a plataforma e envolve, sempre que aplicável, no mínimo:

1.10.2.1 Inclusão das informações dos servidores da contratada em listas de permissão (*whitelisting*) do Tribunal Regional Eleitoral do Rio Grande do Norte.

1.10.2.2 Configuração da integração com *Active Directory* e ADFS.

1.10.2.3 Carregamento dos usuários (extraídos do AD) e classificação em grupos.

1.10.2.4 Habilitação de Duplo Fator de Autenticação.

1.10.3 Toda instrução e passagem de conhecimento (repasse tecnológico) é aberta ao quantitativo de profissionais necessários para gestão da plataforma, a critério do Tribunal Regional Eleitoral do Rio Grande do Norte.

1.10.4 Deverá ser agendada, no mínimo, uma reunião por videoconferência entre o gerente de contas e os

administradores do Tribunal Regional Eleitoral do Rio Grande do Norte para o repasse tecnológico, durante o período de *onboarding*:

1.10.4.1 O repasse tecnológico deve envolver, no mínimo:

1.10.4.1.1 Melhores práticas para implantação.

1.10.4.1.2 Forma de acesso dos usuários e *download* de conteúdos.

1.10.4.1.3 Criação de grupos inteligentes.

1.10.4.1.4 Atribuição de treinamentos a grupos de usuários.

1.10.4.1.5 Carga de conteúdos do Tribunal Regional Eleitoral do Rio Grande do Norte.

1.10.4.1.6 Criação e automatização de campanhas de *phishing*.

1.10.4.1.7 Criação de *roles* (papéis) de segurança.

1.10.4.1.8 Carga, inativação e exclusão de usuários.

1.10.4.1.9 Personalização de identidade visual.

1.10.4.1.10 Emissão e extração de relatórios.

1.10.4.2 O Tribunal Regional Eleitoral do Rio Grande do Norte poderá ainda, a seu critério, solicitar a inclusão de qualquer outro tema relacionado às especificações constantes neste estudo.

1.10.5 A critério do Tribunal Regional Eleitoral do Rio Grande do Norte, poderão serem solicitadas outras reuniões por videoconferência com o gerente de contas durante a vigência da contratação.

1.11 DE GARANTIA E MANUTENÇÃO

1.11.1 Os softwares e licenças fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório do *software*, conforme Art. 73, I, “a”, da Lei 8.666/1993.

1.11.2 O suporte pelo fabricante será obrigatório.

1.11.2.1 Durante todo o período da contratação deverá haver um profissional especializado apto a prestar suporte aos gestores da plataforma no esclarecimento de dúvidas.

1.11.2.2 O profissional deverá estar acessível no período 8hx5d, dias úteis.

1.11.3 O suporte pela fornecedora da solução será opcional e ela poderá subcontratar uma empresa autorizada pelo fabricante para prestar o suporte técnico de primeiro nível.

1.11.4 A fornecedora da solução deverá indicar, na assinatura da contratação, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos produtos ou diretamente com o fabricante.

1.11.4.1 A empresa fornecedora da solução ou o fabricante deverão disponibilizar, cumulativamente, abertura de suporte técnico por meio de atendimento telefônico, *website* e e-mail.

1.11.4.2 Os chamados telefônicos deverão estar disponibilizados de segunda-feira a sexta-feira, das 8 às 18 horas, adotando-se para tanto o horário de Brasília.

1.11.5 A empresa deverá possuir, no momento da assinatura da contratação, pelo menos **01 (um)**

profissional com certificação técnica emitida pelo fabricante, capaz de prestar o serviço especializado de instalação e configuração da solução.

1.11.6 Os serviços de garantia aos produtos deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio fabricante dos produtos fornecidos.

1.12 DE CAPACITAÇÃO

1.12.1 Deverá ser realizado o repasse tecnológico para a equipe técnica por meio presencial ou remotamente, e deverá abordar as informações necessárias à gerência, administração, auditoria e suporte interno da solução.

1.12.2 Além do repasse tecnológico para as equipes técnicas, deverão ser fornecidos documentos e tutoriais (em português) necessários à capacitação dos usuários finais a respeito das funcionalidades da solução.

1.13 DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.13.1 Os serviços previstos objeto deste estudo preliminar deverão ser realizados por profissionais com perfis técnicos compatíveis com cada atividade, ou seja, por recursos especialistas habilitados, com base em cursos e certificações oficiais.

1.14 DE FORMAÇÃO DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.14.1 Não se aplica.

1.15 DE METODOLOGIA DE TRABALHO

1.15.1 Não se aplica.

1.16 DE SEGURANÇA DA INFORMAÇÃO

- 1.16.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL e, em especial, observar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituída através da Resolução no 23.501 de 19 de dezembro de 2016 do Tribunal Superior Eleitoral e a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, instituída através da Resolução nº 20/2019 de 11 de setembro de 2019, quanto aos seguintes aspectos:
- 1.16.1.1 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 Rio Grande do Norte aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.
- 1.16.1.2 O Tribunal Regional Eleitoral do Rio Grande do Norte terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.
- 1.16.1.3 Os documentos eventualmente produzidos deverão ser repassados ao Tribunal Regional Eleitoral do Rio Grande do Norte tanto em formato não editável (*PDF*) como também em formato editável (*.DOCX* ou *.ODT*).
- 1.16.2 A fornecedora da solução deverá concordar que as informações a que terá acesso serão utilizadas somente nos processos envolvidos para execução do objeto contratado.
- 1.16.3 A fornecedora da solução se obriga a informar imediatamente ao Tribunal Regional Eleitoral do Rio Grande do Norte qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.
- 1.16.4 A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do Tribunal Regional Eleitoral do Rio Grande do Norte por ela gerenciadas e armazenadas.
- 1.16.5 O acesso as ferramentas de colaboração e comunicação deverá ser feito através de conexão segura (*HTTPS*).
- 1.16.6 Garantir a segurança das informações dos usuários carregadas na plataforma.
- 1.16.7 Garantir que as informações produzidas no decorrer do programa não sejam perdidas por interrupção ou término da contratação.

1.17 DE QUALIDADE

- 1.17.1 Não se aplica.

2 AVALIAÇÃO DE SOLUÇÕES

2.1 DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA

2.1.1 Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

2.2 DISPONIBILIDADE SOLUÇÕES EXISTENTES NO PORTAL DO SOFTWARE PÚBLICO BRASILEIRO

2.2.1 Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

2.3 CAPACIDADE E ALTERNATIVAS NO MERCADO DE TIC, INCLUSIVE A EXISTÊNCIA DE SOFTWARE LIVRE OU SOFTWARE PÚBLICO

2.3.1 Com base nos requisitos funcionais, buscou-se no mercado plataformas de capacitação em segurança da informação que fossem aderentes às necessidades, assim, buscou-se empresas/soluções que:

2.3.1.1 Fossem notoriamente reconhecidas nesse campo de atuação – conscientização em segurança da informação.

2.3.1.2 Disponibilizassem a maior biblioteca de conscientização e capacitação em português (em linguagem nativa ou legendado).

2.3.1.3 Agregassem o recurso prático de treinamento dos usuários através de simulações de *phishing*, que é, hoje, a técnica de engenharia social mais usada por invasores contra os usuários de tecnologia da informação.

2.3.1.4 Permitissem a integração de conteúdo da Justiça Eleitoral, a exemplo de treinamentos de capacitação já produzidos por alguns Regionais, como Minas Gerais, Pernambuco e Rio Grande do Norte, o que permite a construção de um ambiente único de treinamento, facilitando os esforços de gestão.

2.3.1.5 Trouxessem o indicador de evolução da maturidade dos usuários e da instituição durante a execução do programa.

2.3.1.6 Disponibilizassem a gestão integrada de todos os recursos.

2.3.1.7 Foram analisadas, a partir das especificações técnicas constantes neste estudo, as plataformas:

| Item | Plataforma |
|-------------|------------------------|
| 2.3.1.7.1 | <i>Hackers Rangers</i> |
| 2.3.1.7.2 | <i>Knowbe4</i> |
| 2.3.1.7.3 | <i>Proofpoint</i> |

2.3.1.8 A tabela abaixo apresenta o resultado da análise:

| Avaliação de plataforma para programa permanente de conscientização em segurança da informação | | | | | |
|--|--|--------------------|-------------------------------|-----------|------------|
| Tema | Característica | Item do ETP | Hackers Rangers | Knowbe4 | ProofPoint |
| Conteúdo Nativo | Conteúdo em língua portuguesa ou legendado em português nacional (300 itens) | 1.8.1.1 | Não (80) | Sim (486) | Sim (403) |
| | Conteúdo LGPD Nacional | 1.8.1.1.1.2 | Sim | Sim | Sim |
| | Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (<i>posteres</i>), assessments (avaliações) | 1.8.1.2 | Sim | Sim | Sim |
| | Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior) | 1.8.1.1.1.1 | N/A | Sim | Sim |
| Conteúdo do Cliente | Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (<i>Moodle</i> , usado pela JE)? | 1.8.1.5 | Parcial/ Não permite scorm | Sim | Não |
| | Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma? | 1.8.1.5.1 | Sim | Sim | Não |
| Implantação e Segurança | Carga de usuários por meio de arquivos csv? | 1.8.1.3.4 | Sim | Sim | Sim |
| | Possui integração com AD? | 1.8.1.3.5 | Sim | Sim | Sim |
| | Permite duplo fator de autenticação para usuários e administradores? | 1.8.1.14 | Não | Sim | Não |
| Normas de Segurança como conteúdo | Formato PDF Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? | 1.8.1.5 1.8.1.6 | Não | Sim | Não |

| Avaliação de plataforma para programa permanente de conscientização em segurança da informação | | | | | |
|--|---|----------------------|--|---------|------------|
| Tema | Característica | Item do ETP | Hackers Rangers | Knowbe4 | ProofPoint |
| Automação | Atribuição automática de treinamento para novos usuários? | 1.8.1.3.2 | Não A plataforma tem como base a gamificação Funciona como um Jogo | Sim | Sim |
| | Criação automatizada de um programa personalizado em segurança da informação ou recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários? | 1.8.1.16 | Não | Sim | Não |
| | APIs que permitam a exportação de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante para guarda ou integração com outros sistemas? | 1.8.1.12 1.8.1.19 | Não | Sim | Sim |

| Tema | Característica | Item do ETP | Hackers Rangers | Knowbe4 | ProofPoint |
|------------------------------------|---|-------------|--------------------------------------|---------|------------|
| Gestão de Usuários e Cursos | Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos) | 1.8.1.3.1 | Não | Sim | Sim |
| | Acompanhamento online de progressão e desempenho dos usuários? | 1.8.1.7 | Sim | Sim | Sim |
| | Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos | 1.8.1.8 | Sim | Sim | Sim |
| | Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos? | 1.8.1.10 | Sim | Sim | Sim |
| | Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes? | 1.8.1.3.3 | Não O administrador manda e-mails | Sim | Sim |
| | Inativação de usuários sem perda do histórico de dados? | 1.8.1.3.6 | | Sim | Sim |
| | Possibilita a atribuição da licença de acesso de um usuário que foi desligado da instituição para um novo usuário (neste caso não é necessário manter o histórico)? | 1.8.1.3.7 | Sim | Sim | Sim |
| | Provê ambiente de gestão que possibilita a criação de grupos de usuários com base em comportamento frente as simulações e treinamentos realizados? | 1.8.1.9 | Sim | Sim | Sim |
| | Emissão de Certificados para os cursos? | 1.8.1.11 | Não | Sim | Sim |
| | Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos? | 1.8.1.13 | Sim | Sim | Sim |

| Avaliação de plataforma para programa permanente de conscientização em segurança da informação | | | | | |
|--|--|-------------|-----------------|---------|------------|
| Tema | Característica | Item do ETP | Hackers Rangers | Knowbe4 | ProofPoint |
| Campanhas de Phishing | Permite a criação de número ilimitado de campanhas durante a vigência da contratação? | 1.8.1.15.1 | Sim | Sim | Sim |
| | Disponibiliza pelo menos 50 (cinquenta) modelos de campanhas em português e permitir a personalização dos modelos pela contratante; | 1.8.1.15.2 | Sim | Sim | Sim |
| | Mantém histórico por usuário e por campanha | 1.8.1.15.3 | Sim | Sim | Sim |
| | Permite que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação? | 1.8.1.15.4 | Sim | Sim | Sim |
| Indicador de Maturidade em Segurança | Possui indicador de nível de risco em segurança da informação para cada usuário e para a instituição? O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de <i>phishing</i> . | 1.8.1.17 | Não | Sim | Não |

| Avaliação de plataforma para programa permanente de conscientização em segurança da informação | | | | | |
|--|---|------------------|-----------------|---------|------------|
| Tema | Característica | Item do ETP | Hackers Rangers | Knowbe4 | ProofPoint |
| Supporte Técnico | A contratada disponibiliza durante todo período contratual um gerente de contas para apoiar e orientar a contratante no uso da plataforma | 1.10.3 1.10.4 | Sim | Sim | Sim |
| | Repasso tecnológico | 1.10.3 | Sim | Sim | Sim |
| Customização | Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários? | 1.10.3.1. 9 | Sim | Sim | Sim |
| Linguagem da Plataforma | Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br) | 1.1.1.1.8 | Sim | Sim | Não |

2.3.1.9 Entre as plataformas analisadas, a plataforma **Knowbe4** foi a que atendeu a todos os requisitos propostos.

2.3.1.10 O Estudo teve por base a comparação as principais soluções, porém entende-se que diante da dinâmica do mercado, a lista pode não ser exaustiva, havendo a possibilidade de existirem outras plataformas que não foram analisadas.

2.3.1.11 Assim, é fundamental que seja devidamente demonstrada a legítima necessidade da Administração em relação às exigências que conduziram a este resultado.

2.3.1.11.1 Importante considerar que a Administração Pública não pode abrir mão de suas necessidades legítimas, com intenção de tornar o procedimento licitatório mais abrangente.

2.3.1.11.2 Fazendo isso o gestor público permitiria que ferramentas mais simples e que atenderiam somente em parte as necessidades da Administração concorressem com soluções integralmente aderentes às necessidades, mais completas e abrangentes.

2.3.1.11.3 Tal cenário criaria, em última análise, uma situação de desigualdade, visto ser alta a probabilidade das soluções totalmente aderentes às reais necessidades da Administração não conseguirem ser competitivas no certame.

2.3.1.12 Assim, não obstante a **Knowbe4** ser a única plataforma do estudo que atende integralmente as exigências, o Termo de Referência não trará indicação de marca, apresentando somente as necessidades da Administração.

2.3.1.13 Isso permitirá ainda que todos os *players* do mercado possam trazer questionamentos que julgarem pertinentes a respeito de qualquer uma das especificações constantes no Termo.

2.3.1.14 Cabe ressaltar finalmente que, mesmo sendo a *Knowbe4* a única a atender todos os requisitos, há no mercado várias empresas que fornecem a solução, permitindo, assim, um certame competitivo.

2.4 OBSERVÂNCIA ÀS POLÍTICAS, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS DEFINIDAS PELOS MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO (MNI) E MODELO DE ACESSIBILIDADE DE GOVERNO ELETRÔNICO (E-MAG)

2.4.1 A solução a ser implantada não tem por finalidade a comunicação com outros órgãos do Poder Judiciário, portanto, não se aplica a observância ao Modelo Nacional de Interoperabilidade MNI.

2.4.2 A solução a ser implantada será acessível somente a determinados servidores do quadro deste Regional, portanto, não se aplica a observância ao Modelo de Acessibilidade de Governo Eletrônico E-MAG.

2.5 OBSERVÂNCIA AOS REQUISITOS ESTABELECIDOS PELA RESOLUÇÃO CNJ Nº 211/2015 E ALTERAÇÕES POSTERIORES, NA CONTRATAÇÃO DE SERVIÇOS DE DESENVOLVIMENTO E DE SUSTENTAÇÃO DE SISTEMAS DE INFORMAÇÃO

2.5.1 Não se aplica.

2.6 ADERÊNCIA ÀS REGULAMENTAÇÕES DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS (ICP-BRASIL), QUANDO HOUVER NECESSIDADE DE UTILIZAÇÃO DE CERTIFICADO DIGITAL, OBSERVADA A LEGISLAÇÃO SOBRE O ASSUNTO

2.6.1 Não se aplica.

2.7 OBSERVÂNCIA ÀS ORIENTAÇÕES, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS E FUNCIONAIS DEFINIDAS PELO MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO DE PROCESSOS E DOCUMENTOS DO PODER JUDICIÁRIO (MOREQ-JUS), DO CONSELHO NACIONAL DE JUSTIÇA – CNJ E PELO E-ARQ (NORMAS E PADRÕES DE ARQUIVOLOGIA)

2.7.1 Não se aplica.

2.8 ORÇAMENTO ESTIMADO QUE EXPRESSE A COMPOSIÇÃO DE TODOS OS CUSTOS UNITÁRIOS RESULTANTES DOS ITENS A SEREM CONTRATADOS, ELABORADO COM BASE EM PESQUISA FUNDAMENTADA DE PREÇOS, COMO OS PRATICADOS NO MERCADO DE TIC EM CONTRATAÇÕES SIMILARES REALIZADAS POR ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA, ENTRE OUTROS PERTINENTES

2.8.1 Em consulta realizada para uma prévia comparação de custos, se obteve o seguinte:

| Item | Descrição | Quantidade | Preço 36 (trinta e seis) meses R\$ | Preço Total R\$ |
|--------------|--|------------|--|-----------------------|
| 1 | Solução para educação e conscientização em segurança da informação | 500 | 119,80 | 59.900,00 |
| Total | | | | 59.900,00 |

3 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

3.1 A solução escolhida foi a alternativa descrita:

- 3.1.1 Inicialmente, no **item 2.3.1.7.1**, para a contratação de licenças de acesso à plataforma integrada de treinamento *online*, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação.
- 3.1.2 Porém, em virtude da aprovação da Estratégia Nacional de Cibersegurança para o período de 2021 a 2024, com o objetivo de servir como direcionador para as diversas ações necessárias em segurança cibernética, foram instituídos diversos grupos de trabalho em Segurança da Informação, dentre eles um para a aquisição da solução, descrita no item anterior (3.1.1), para toda Justiça Eleitoral.

3.1.3 A alternativa que oferece mais vantajosidade para o Tribunal Regional Eleitoral do Rio Grande do Norte é a de atuar como partícipe da Ata de Registro de Preços (ARP), atualmente, em curso no Tribunal Regional Eleitoral do Espírito Santo (TRE/ES).

3.2 Justificativa da escolha:

- 3.2.1 A Ata de Registro de Preços (ARP) para a contratação de serviço de conteúdo na modalidade “Software as Service” (SaaS) para treinamento dos usuários, por meio do acesso à plataforma *online*, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação, do Tribunal Regional Eleitoral do Espírito Santo, atende a todos os requisitos elencados neste estudo, onde o processo está finalizado e se configuraria a solução mais vantajosa, caso o Tribunal Regional Eleitoral do Rio Grande do Norte opte por participar do referido registro de preços.

- 3.2.2 O processo em curso contemplará, além das necessidades do TRE/ES, as demandas dos demais Tribunais Eleitorais interessados, que integrarão a contratação como partícipes desde a origem.

3.2.2.1 Esta ata de registro de preços é composta por:

| Item | Descrição | Quantidade | Valor Unitário Registrado |
|-------------|--|-------------------|----------------------------------|
| 1 | Contratação de licenças de acesso à plataforma integrada de treinamento online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, com validade de 36 (trinta e seis) meses | 25.730 | R\$ 99,99 |

3.3 A solução está alinhada:

3.3.1 Às necessidades de negócio e requisitos tecnológicos.

3.3.2 Necessidade de alcance dos seguintes objetivos estratégicos, elencados no:

3.3.2.1 Plano Estratégico da Justiça Eleitoral do RN 2021-2026 (PEJERN):

3.3.2.1.1 Fortalecimento da segurança da informação – Objetivo Estratégico AC3.

3.3.2.1.1.1 Promover o fortalecimento contínuo da segurança da informação no âmbito institucional – Iniciativa AC3.1.

3.3.2.1.1.2 Fortalecer a segurança cibernética assegurando o alinhamento às diretrizes do Poder Judiciário – Iniciativa AC3.2.

3.3.2.1.1.3 Aprimorar a infraestrutura tecnológica e os serviços em nuvem – Iniciativa AC3.3.

3.3.2.1.1.4 Fortalecer a gestão de riscos de incidentes de TIC – Iniciativa AC3.4.

3.3.2.1.1.5 Implementar mecanismos voltados à proteção de dados pessoais – Iniciativa AC3.5.

3.3.2.2 Plano Diretor de Tecnologia da Informação e Comunicação 2021-2022 (PDTIC):

3.3.2.2.1 Aprimorar a segurança da informação e gestão de dados – Objetivo Estratégico OE7 – Camada 1.

3.3.2.2.2 Aprimorar protocolos de cibersegurança – Objetivo Tático OT7.1 – Camada 2.

3.3.2.2.3 Aprimorar controles de segurança e proteção de dados pessoais – Objetivo Tático OT7.2 – Camada 2.

3.3.2.2.4 Promover serviços de infraestrutura e soluções corporativas – Objetivo Estratégico OE8 – Camada 1.

3.3.2.2.5 Prover soluções e serviços de infraestrutura com capacidade, disponibilidade e desempenho adequados – Objetivo Estratégico OT8.2 – Camada 2.

3.4 A solução escolhida permitirá:

3.4.1 Tornar-se um dos pilares para a execução de um programa permanente de conscientização em segurança da informação na Justiça Eleitoral, com os seguintes recursos:

3.4.1.1 Disponibilizará ampla biblioteca de conteúdos de segurança da informação, inclusive LGPD, em língua portuguesa.

3.4.1.2 Entregará conhecimento com uso de recursos interativos, como vídeo, simulações, quizzes (questionários rápidos), boletins informativos, etc.

3.4.1.3 Possibilitará a inclusão de cursos produzidos pela própria Justiça Eleitoral ou por terceiros, gerenciando-os com os conteúdos nativos da solução.

3.4.1.4 Permitirá a execução de campanhas e simulações de treinamento automatizadas, em especial, simulações de *phishing* (mensagens eletrônicas que são armadilhas para roubar dados e inserir vírus na rede).

3.4.1.5 Permitirá o carregamento de políticas e normas de segurança da Justiça Eleitoral como conteúdo, a fim de que os usuários estudem (leiam) e efetuem o aceite.

3.4.1.6 Permitirá o acompanhamento da evolução da maturidade dos usuários e da instituição em relação a Segurança da Informação.

3.4.1.7 Permitirá a gestão completa de treinamento e usuários.

3.4.1.8 Permitirá a integração com a base de dados de usuários do órgão.

3.5 Os valores estimados estão descritos no item 2.8.1.

3.6 Os benefícios gerados são:

3.6.1 Treinar e conscientizar os servidores da Justiça Eleitoral, visando o fortalecimento da segurança da infraestrutura tecnológica e dos dados pessoais da instituição.

3.6.2 Manter o ambiente computacional da Justiça Eleitoral seguro.

3.6.3 Proteção dos usuários, da instituição e da propriedade intelectual.

3.6.4 Manter uma infraestrutura tecnológica de cibersegurança, priorizando as ferramentas elencadas no rol de soluções tecnológicas que foi elaborado para atender à Estratégia de Cibersegurança da Justiça Eleitoral, de acordo com os níveis de criticidade pré-definidos, alinhado com as necessidades do TRE/RN e de acordo com a sua capacidade operacional.

3.6.5 Permitir, conforme a solução esteja sendo implementada, que os processos de trabalho sejam documentados, bem como que padrões e boas práticas de operação, suporte e manutenção sejam criados e se tornem disponíveis com acesso restrito às equipes técnicas e de gestão responsáveis.

3.6.6 Garantir a uniformidade do parque tecnológico em âmbito nacional, baseado em levantamento realizado junto aos Tribunais Eleitorais (TSE e TREs), permitindo a possibilidade de agrupamento de Tribunais para aquisições em conjunto, facilitando a troca de informações e uma melhor gestão das equipes técnicas envolvidas.

3.6.7 Permitir o monitoramento de anomalias e ataques cibernéticos ao ambiente computacional da Justiça Eleitoral.

3.6.8 Aumentar a resiliência da Justiça Eleitoral.

3.7 Relação Demanda Prevista x Quantidade de Bens Pretendidos (memória de cálculo):

3.7.1 Atualmente, considerando o aspecto orçamentário, a necessidade será atendida pela contratação de licenças do(s) seguinte(s) software(s), na(s) quantidade(s) indicada(s):

| Descrição | Quantidade Atual | Quantidade Necessária (Projeção) | Quantidade para Aquisição |
|--|-----------------------------|---|--------------------------------------|
| Contratação de licenças de acesso à plataforma integrada de treinamento online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, com validade de 36 (trinta e seis) meses | 0 | 500 | 1.000 |

4 NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

4.1 Não existe necessidade de adequação do ambiente para a execução contratual.

II – SUSTENTAÇÃO DA CONTRATAÇÃO

5 DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

5.1 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.1.1 Gestão da Plataforma de Conscientização.

5.1.1.1 Haverá necessidade de gestão da plataforma em relação aos treinamentos e às campanhas de *phishing*.

5.1.1.2 Desde a concepção, essa contratação integra as equipes responsáveis pela capacitação de servidores e tecnologia da informação tendo, inclusive, servidores dessas duas áreas na elaboração dos documentos de planejamento da contratação.

5.1.1.3 Na execução do programa, é altamente recomendável que:

5.1.1.3.1 A gestão dos treinamentos fique a cargo da área responsável pela capacitação de servidores, com apoio da área tecnologia da informação, quanto a construção do programa de capacitação em Segurança da Informação.

5.1.1.3.2 A gestão de eventuais treinamentos adicionais a serem adicionados na plataforma fique a cargo da área responsável pela capacitação de servidores.

5.1.1.3.3 A gestão das campanhas de *phishing* fiquem a cargo da área de tecnologia da informação.

5.1.1.4 A gestão da plataforma terá sempre o apoio do Gerente de Contas da Contratada, conforme atribuições definidas neste estudo.

5.1.2 Gestão do Programa de Conscientização em Segurança da Informação.

5.1.2.1 É altamente recomendável que as áreas de gestão de pessoas (responsável pela capacitação de servidores) e tecnologia da informação definam um cronograma de treinamentos e testes de *phishing*, com periodicidade máxima semestral e busque o apoio da alta administração para efetivar a execução junto aos usuários finais.

5.1.2.2 Como está sendo contratada uma plataforma única para toda a Justiça Eleitoral, uma solução viável para conduzir o programa seria a formalização de uma comissão nacional, com participação das áreas de gestão de pessoas (responsável pela capacitação de servidores) e tecnologia da informação, visando a elaboração de um cronograma de treinamentos e testes que poderia ser usado por todos os Tribunais que tivessem interesse.

5.1.2.2.1 Essa ação otimizaria os recursos humanos e contribuiria para uma evolução de maturidade similar em toda a justiça eleitoral.

5.2 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.2.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a implantação da solução.

5.3 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.3.1 Não foi identificada a necessidade de recursos humanos adicionais para garantir a continuidade da solução.

5.4 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.4.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a continuidade da solução.

6 DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DA CONTRATAÇÃO

6.1 Não se aplica.

7 ELABORAÇÃO DE ESTRATÉGIA DE INDEPENDÊNCIA

7.1 TRANSFERÊNCIA DE CONHECIMENTO TECNOLÓGICO

7.1.1 Não se aplica.

7.2 DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS

7.2.1 Não se aplica.

7.3 DOCUMENTAÇÃO E AFINS PERTINENTES À TECNOLOGIA DE CONCEPÇÃO, MANUTENÇÃO, ATUALIZAÇÃO E CÓDIGO FONTE

7.3.1 Não se aplica.

III – ANÁLISE DE RISCOS

8 IDENTIFICAÇÃO DOS RISCOS

8.1 RISCOS DO PROCESSO DE CONTRATAÇÃO

| Risco | 8.1.1 Indisponibilidade Orçamentária | Probabilidade: | MÉDIA |
|---|--|----------------|----------|
| Item | Dano | | Impacto: |
| 1 | Não contratação imediata da solução | | ALTO |
| 2 | Atraso no cronograma | | MÉDIO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | Responsável | |
| 1 | Verificar e confirmar previamente disponibilidade orçamentária para a contratação da solução pretendida | STIE | |
| 2 | Encaminhar em tempo hábil proposta de dotação orçamentária ao Órgão Ordenador de Despesas com previsão e prazo para a contratação da solução | STIE | |
| Item | Corretiva | Responsável | |
| 1 | Solicitar o remanejamento de recursos para atender temporariamente o serviço objeto do Termo de Referência | STIE | |

| Risco | 8.1.1 Atraso no Trâmite Processual | Probabilidade: | MÉDIA |
|---|--|---------------------------------------|----------|
| Item | Dano | | Impacto: |
| 1 | Atraso na contratação da solução | | MÉDIO |
| 2 | Atraso no cronograma | | MÉDIO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | Responsável | |
| 1 | Finalizar o Termo de Referência e documentos acessórios respeitando o cronograma previamente definido | Equipe de Planejamento da Contratação | |
| 2 | Comunicar à Administração da criticidade do objeto contratado e da necessidade de agilidade na análise dos documentos e na tramitação do processo administrativo | STIE | |
| Item | Corretiva | Responsável | |
| 1 | Comunicar à Administração sobre a paralisação do processo durante a tramitação e solicitar prioridade na análise visando à conclusão do processo administrativo | STIE | |

| Risco | 8.1.2 Impugnação Procedente | Probabilidade: | BAIXA |
|---|---|---------------------------------------|-------|
| Item | Dano | Impacto: | |
| 1 | Interrupção do processo de contratação | ALTO | |
| 2 | Atraso no cronograma | ALTO | |
| 3 | Frustração da contratação | ALTO | |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | Responsável | |
| 1 | Elaboração de Estudos Preliminares e Termo de Referências consistentes que permitam assegurar a contratação | Equipe de Planejamento da Contratação | |
| 2 | Revisar o Termo de Referência e certificar que o mesmo não possua cláusulas que restrinjam, sem a devida justificativa técnica, a participação de interessados ou que, de alguma forma, deixem um licitante em situação privilegiada para concorrer | Equipe de Planejamento da Contratação | |
| 3 | Submeter, para análise, o Termo de Referência à Administração | Equipe de Planejamento da Contratação | |
| 4 | Atendimento imediato por parte do suporte técnico a fim de responder, tempestivamente, os pedidos de esclarecimentos e impugnações apresentadas | Equipe de Planejamento da Contratação | |
| Item | Corretiva | Responsável | |
| 1 | Adequação do Termo de Referência, corrigindo os itens que foram motivos de impugnação, para viabilizar a reabertura do certame. | Equipe de Planejamento da Contratação | |
| 2 | Promover a reabertura da licitação | Área Administrativa | |

| | | | |
|---|--|-----------------------|---------------------------------------|
| Risco | 8.1.3 Licitação Frustrada (Deserta/Fracassada) | Probabilidade: | BAIXA |
| Item | Dano | | Impacto: |
| 1 | Interrupção do processo de contratação | | ALTO |
| 2 | Atraso no cronograma | | ALTO |
| 3 | Frustração da contratação | | ALTO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | | Responsável |
| 1 | Promover análise de mercado com o objetivo de elencar as empresas que prestam serviço do objeto | | Equipe de Planejamento da Contratação |
| 2 | Dar a devida publicidade ao certame licitatório | | Área Administrativa |
| 3 | Evitar exigências técnicas demasiadamente restritivas e desnecessárias | | Equipe de Planejamento da Contratação |
| 4 | Mensurar o preço global do serviço a ser contratado através de estudo minucioso, com pesquisa de preços na Internet, bem como com prestadores de serviço do ramo | | Equipe de Planejamento da Contratação |
| Item | Corretiva | | Responsável |
| 1 | Adequação do Termo de Referência para a realização de novo certame | | Equipe de Planejamento da Contratação |
| 2 | Promover nova licitação | | Área Administrativa |
| 3 | Pesquisa de Preços, caso necessário | | Equipe de Planejamento da Contratação |
| 4 | Contratação Direta | | Área Administrativa |

| | | | |
|---|---|-----------------------|---------------------------------------|
| Risco | 8.1.4 Licitação Anulada | Probabilidade: | BAIXA |
| Item | Dano | | Impacto: |
| 1 | Interrupção do processo de contratação | | ALTO |
| 2 | Atraso no cronograma | | ALTO |
| 3 | Frustração da contratação | | ALTO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | | Responsável |
| 1 | Na elaboração do Termo de Referência observar se não existe vício de legalidade | | Equipe de Planejamento da Contratação |
| 2 | Observar adequada publicidade da licitação | | Área Administrativa |
| Item | Corretiva | | Responsável |
| 1 | Adequação das exigências normativas sobre o objeto/procedimento licitatório | | Equipe de Planejamento da Contratação |
| 2 | Promover a publicidade adequada à modalidade de licitação escolhida | | Área Administrativa |

8.2 RISCOS DA SOLUÇÃO DE TID (GESTÃO E EXECUÇÃO CONTRATUAL)

| Risco | 8.2.1 Solução considerada inadequada pela área requisitante | Probabilidade: | BAIXA |
|--|--|---------------------|-------|
| Item | Dano | Impacto: | |
| 1 | Insatisfação dos usuários dos serviços de TIC | ALTO | |
| 2 | Não utilização da solução | ALTO | |
| 3 | Necessidade de nova avaliação da solução | MÉDIO | |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | Responsável | |
| 1 | Envolver o usuário/unidade requisitante na participação em todas as fases da contratação | STIE e SAOF | |
| 2 | Nomear servidores experientes e capacitados para executar a fase de levantamento de requisitos da solução de TIC | STIE | |
| Item | Corretiva | Responsável | |
| 1 | Nomear nova Equipe de Planejamento da Contratação, substituindo a atual, para a elaboração de novo Termo de Referência visando a contratação de solução de TIC adequada a solicitação da área demandante | Área Administrativa | |
| 2 | Nomear equipe ou realocar servidores do Tribunal Regional Eleitoral do Rio Grande do Norte com o objetivo de auxiliar ou assumir, provisoriamente, a operação dos serviços prestados pela equipe da fornecedora da solução | STIE | |
| 3 | Refazer o levantamento de requisitos junto ao usuário/unidade requisitante | STIE | |
| 4 | Proceder com as alterações necessárias, na medida do possível, na solução de TIC fornecedora da solução, com objetivo de readequar e reimplantar a solução | STIE | |

| | | | |
|---|--|-----------------------|---------------------|
| Risco | 8.2.2 Não cumprimento do prazo de entrega da solução | Probabilidade: | BAIXA |
| Item | Dano | Impacto: | |
| 1 | Atraso na instalação da(s) licença(s) | | BAIXO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | | Responsável |
| 1 | Consultar as empresas do ramo sobre adequação do prazo de entrega da solução | | STIE |
| 2 | Acompanhar rigorosamente junto à empresa o andamento da operação de entrega | | Área Administrativa |
| Item | Corretiva | | Responsável |
| 1 | Solicitar o fornecedor para a entrega imediata | | Área Administrativa |
| 2 | Verificar as sanções cabíveis no caso do não cumprimento do prazo de entrega | | Área Administrativa |

| | | | |
|---|--|-----------------------|--------------------|
| Risco | 8.2.2 Entrega da solução incompatível (especificações) | Probabilidade: | BAIXA |
| Item | Dano | Impacto: | |
| 1 | Ineficácia na execução dos serviços prestados pelo Órgão | | ALTO |
| Ações de Prevenção/Contingência e Responsáveis | | | |
| Item | Preventiva | | Responsável |
| 1 | Verificar se o software está de acordo com as especificações mínimas exigidas no ato de entrega para fins de ateste provisório | | STIE |
| Item | Corretiva | | Responsável |
| 1 | Solicitar o fornecedor para a substituição do software incompatível | | STIE |
| 2 | Informar o gestor da contratação sobre problemas contratuais de garantia | | STIE |

IV – CONCLUSÃO DOS ESTUDOS PRELIMINARES

9 DECLARAÇÃO DE VIABILIDADE

Em conformidade com o disposto no Manual de Contratações de Tecnologia da Informação e Comunicação, subitem 4.1.1.11, DECLARAMOS a viabilidade da contratação, com base no estudo realizado.

Natal/RN, (*datação eletrônica*)

Equipe de Planejamento da Contratação

| Integrante Demandante | Integrante Técnico |
|---|--|
| (assinado eletronicamente) Carlos Magno do R Câmara COINF/STIE | (assinado eletronicamente) Francisco de Assis Paiva Leal SSI/COINF/STIE |