Poder Judiciário
Tribunal Regional Eleitoral da Bahia

Estudos Preliminares

Contratação de Consultoria para implantação de um Sistema de Gestão da Segurança da Informação e Privacidade (SGSI/SGPI) e obtenção da certificação do TRE-BA nas ISO 27.001 e 27.701

Integrantes da Equipe de Planejamento da Contratação			
Papel	**Nome Completo**	**Lotação**	**Ramal**
Integrante Demandante	ANDRÉA OLIVEIRA ALMEIDA QUEIROZ	SEAGG	9231
Integrante Técnico	RILSON BARROS DE ALMEIDA	SEINFRA	7395
Integrante Administrativo	ONEÍZA MABEL CARNEIRO GUEDES	GAB-SJU	7163

Versão deste documento 1.0
Data 11/03/2022

SUMÁRIO

1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

Contextualização

O Plano Estratégico Institucional (PEI) 2021-2026 do Tribunal Regional Eleitoral da Bahia estabelece como um dos seus objetivos estratégicos "Promover a Melhoria Contínua da Governança e da Gestão de TIC", a qual prevê a busca continua da inovação tecnológica, aprimoramento dos processos de trabalho de TIC, promover a satisfação dos usuários, aperfeiçoando a infraestrutura tecnológica e a gestão da segurança da informação e da proteção de dados pessoais, dentre outros. Apresenta ainda, como um dos valores organizacionais, a "Segurança", firmando o compromisso com a melhoria contínua da segurança nos procedimentos eleitorais, administrativos e naqueles que envolvam fluxo de informações e a proteção de dados institucionais e pessoais.

Impende esclarecer que informação é um ativo essencial a todas as organizações, por isso deve ser protegida adequadamente do crescente aumento de ameaças e vulnerabilidades que possam comprometê-la. Logo, é imprescindível a adoção de medidas que garantam a segurança e a privacidade da informação, reduzindo os riscos e garantindo a continuidade do negócio.

É cediço que a equipe interna da STI não possui conhecimentos técnicos suficientes relativos ao tema em tela. Assim, é necessário contratar uma consultoria técnica especializada que possa planejar, orientar e ajudar na implementação de um Sistema de Gestão da Segurança da Informação e Privacidade (SGSI/SGPI) no TRE-BA, bem como nortear o atendimento aos requisitos das normas ISO 27001 e 27701, visando alcançar altos índices de disponibilidade, integridade e confidencialidade.

A sigla **ISO** significa *International Organization for Standardization* (Organização Internacional de Padronização, em português).

A **ISO** é uma organização fundada em 1946, com sede em Genebra (Suíça) e formada por representantes de 91 países, tendo como principal objetivo promover o desenvolvimento de normas, impulsionando o comércio de bens e serviços. Em outras palavras, serve para normalizar a utilização de produtos e serviços, fazendo o uso de normas que visam a melhoria da qualidade.

No Brasil, é representada pela Associação Brasileira de Normas Técnicas, **ABNT BR**.

A sigla IEC significa *International Electrotechnical Commission*. A IEC é a organização mundial líder que prepara e publica Normas Internacionais para as áreas elétrica, eletrônica e tecnologia.

A **ISO 27001** é a norma padrão de referência para um Sistema de Gestão da Segurança da Informação (SGSI). Ela foi publicada pela ISO e pelo IEC, assim ela também é chamada de ISO/IEC 27001. Tem como foco os princípios basilares da Segurança da Informação (confidencialidade, integridade e disponibilidade da informação). A implementação da ISO 27001 busca garantir o compromisso com a proteção da informação, fornecendo às organizações um modelo de melhores práticas para identificar, analisar e implementar controles para gerenciar riscos de segurança da informação e proteger a confidencialidade, integridade e disponibilidade de dados essenciais aos negócios.

A **ISO 27701 é** uma extensão da ISO 27001, focada em gestão de privacidade de dados. Seu principal objetivo é definir os requisitos adicionais à norma de segurança, de modo que o tratamento das informações considere a questão da privacidade das mesmas.

Enquanto a ISO 27001 estabelece os controles necessários para uma adequada gestão de segurança da informação, a ISO 27701 trata especificamente das questões relacionadas à privacidade, trazendo para isso controles adicionais à ISO 27001. Ou seja, a implantação da 27701 depende da implantação 27001.

A correta implementação das normas pode alavancar significativamente o progresso da organização, proporcionando, dentre outros, os seguintes benefícios:

- **Melhoria Contínua**: Identificação contínua de oportunidades para melhoria. A implementação dos controles provenientes da norma e da análise de risco melhora o desempenho operacional das organizações.
- **Conformidade**: demonstra elevado compromisso com a proteção da informação, garantia de conformidade com a legislação de privacidade e proteção de dados pessoais.
- **Melhor relacionamento entre organização e cliente**: a confiabilidade e satisfação dos clientes em relação à empresa aumenta consideravelmente, providenciando um maior potencial para realização de oportunidades de negócios.
- **Redução de Custos**: Garante a realização de investimentos mais eficientes e orientados ao risco, ao invés de investimentos apenas baseados em tendências.
- **Reconhecimento nacional e internacional à preocupação com a segurança da informação**: demonstra o compromisso da organização para com a segurança da informação, o que representa um nível considerável de conforto para as organizações que interagem com a organização certificada.

1.1 Definição e Especificação dos Requisitos da Demanda

Serviço de consultoria para implantação de um Sistema de Gestão da Segurança da Informação e Privacidade (SGSI/SGPI) no âmbito do TRE-BA, em conformidade com as normas ISO 27.001 e 27.701, bem como prestação de serviço de suporte ao processo de auditoria externa visando à certificação do TRE-BA nas normas citadas. A empresa deverá analisar as normas vigentes no TRE-BA e propor ajustes ou melhorias, além de identificar lacunas no estado atual.

A consultoria inclui ainda, os serviços de planejamento, fortalecimento e treinamento em segurança da informação no âmbito da Secretaria de Tecnologia da Informação e Comunicação.

1.1.1 Requisitos Não Funcionais

a) De Capacitação

Envolve o treinamento dos clientes internos (em especial os gestores de TI do Tribunal, e outros que possam atuar como multiplicadores junto aos demais servidores) nos conceitos de Segurança da Informação e Privacidade, a fim de alinhamento interno do entendimento.

b) Legais

O prestador de serviço deverá ser empresa confiável e sólida, bem como deverá possuir qualificação e experiência no negócio, para assegurar o cumprimento das melhores práticas e conformidade com as normas.

Aqui é importante ressaltar que o processo de **implementação** e **certificação** são realizados por empresas diferentes. Após a implementação, é preciso buscar um órgão certificador que irá realizar auditoria para verificar se os procedimentos implementados estão de acordo com as normas da ISO e emitir a(s) certificação(ões).

Além das orientações expressas nas normas ISO 27001 e 27701, a empresa deverá seguir as diretrizes do CNJ para Gestão de Segurança da Informação no âmbito do Poder Judiciário, a exemplo das Resoluções CNJ nº 370/2021 e 396/2021, além de normativos específicos para a Justiça Eleitoral e de normas de segurança do próprio TRE/BA.

c) De Manutenção

Não se aplica, por se tratar de um processo de melhoria contínua.

d) Temporais

Não se aplica.

e) De Segurança da Informação

A contratada deverá manter sigilo com relação às informações coletadas, em especial as que envolvam o diagnóstico da situação atual do Tribunal.

f) Sociais, Ambientais e Culturais

Não requeridos.

1.1.2 Requisitos Tecnológicos

a) De Arquitetura

Não se aplica.

b) Do Projeto de Implantação da STIC

A implantação deverá ser iniciada e concluída neste exercício.

c) De garantia e Manutenção

Não se aplica.

d) De Capacitação

Não haverá necessidade de capacitação técnica.

e) De Experiência Profissional e Formação da Equipe que Projetará, Implantará e Manterá a STIC

Por se tratar de um processo de melhoria contínua, a contratada deverá promover a capacitação da equipe do TRE visando à manutenção da conformidade com as normas ISO.

f) De metodologia de Trabalho

Não se aplica.

g) De segurança em TIC (confidencialidade, integridade e disponibilidade)

Possuir termo de confidencialidade e de conduta assinado com o Tribunal.

1.2 Identificação de Soluções que Atendem aos Requisitos

1.2.1 Soluções Disponíveis no Mercado de TIC e/ou Contratadas por Outros Órgãos

SOLUÇÃO 1 – Contratação de Consultoria para implementação das certificações ISO 27001 e 27701 no TRE-BA.

Descrição: Contratação de empresa com qualificação e experiência na implantação de SGSI e na certificação nas normas ISO 27.001 e 27.701.

Fornecedor(es): Por se tratar de serviço de consultoria, qualquer empresa capacitada que possua profissionais especializados (certificados) para o escopo desta contratação pode ser contratada.

SOLUÇÃO 2 – Capacitação dos servidores da STI para desenvolvimento de um sistema de segurança da informação.

Descrição: Contratação de empresa para treinamento em segurança da informação no âmbito da Secretaria de Tecnologia da Informação e Comunicação, com foco na implantação de SGSI e nas normas da ISO 27.001 e 27.701.

Fornecedor(es): Qualquer empresa que possua profissionais capacitados/especializados (certificados) para o escopo desta contratação pode ser contratada.

Modelo Nacional de Interoperabilidade – MNI[1]

Não se aplica.

Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil

Não se aplica.

[1] O Modelo Nacional de Interoperabilidade (MNI) visa estabelecer os padrões para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, e além de servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual. (http://www.cnj.jus.br/tecnologia-da-informacao/comite-nacional-da-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade)

Modelo de Requisitos Moreq-Jus[2]

Não se aplica.

Modelo Nacional de Interoperabilidade – MNI

Não se aplica.

Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil

Não se aplica.

Modelo de Requisitos Moreq-Jus

Não se aplica.

1.3 Análise dos Custos Totais da Demanda

Inicialmente, cabe ressaltar que a STI possui uma equipe técnica bastante reduzida, com sobrecarga de serviços, o que dificultaria tanto a capacitação dos servidores, como a elaboração e implementação do SGSI em tempo hábil no exercício. Por esse motivo, a solução 2 não é indicada.

Isto posto, por se constituir o objeto da contratação de demandas específicas (consultoria para diagnóstico e conformidade com normas ISO e capacitação de servidores), optou-se pela solução 1, e foram obtidas as cotações abaixo:

Tabela 1. Cotações

Cotação	Empresa	Valor
1	ITPartners	R$173.800,00 (Consultoria+Apoio à implementação ISO 27001/27701)
2	ITPartners	R$176.526,00 (Licença pelo período de 12 meses da solução – Gestão de Programa de Privacidade)
3	ABNT	R$45.000,00 Auditoria externa para certificação

[2] O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) apresenta os requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir, no intuito de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas. (http://www.cnj.jus.br/programas-e-acoes/pj-proname/sistema-moreq-jus)

1.4 Escolha e Justificativa da Solução

1.4.1 Descrição da Solução

A obtenção das certificações almejadas visa garantir a conformidade do TRE-BA com relação às boas práticas em Segurança da Informação.

1.4.2 Alinhamento da Solução

A solução está alinhada com os objetivos estratégicos de "Aperfeiçoar a Governança e a Gestão Administrativa" e "Promover a melhoria contínua da Governança e da Gestão de TIC" do Planejamento Estratégico Institucional (PEI) do TRE-BA - 2021-2026.

1.4.3 Benefícios Esperados

Criação do Sistema de Gestão da Segurança da Informação no âmbito do TRE-BA e obtenção das Certificações ISO 27.001 e 27.701.

1.4.4 Relação Demanda/Quantidade

A quantidade de meses previstos é suficiente para a contatada realizar o diagnóstico, propor adequação das normas existentes, orientar todo o processo de conformidade com a ISO, implantar requisitos de segurança e realizar treinamentos.

1.5 Adequação do Ambiente

Não se aplica.

2 SUSTENTAÇÃO DO CONTRATO

2.1 Recursos Materiais e de Pessoal

Não há necessidade de obtenção de recursos materiais e de pessoal para a aquisição.

2.2 Continuidade Contratual

Não se aplica.

2.3 Transição e Encerramento Contratuais

Não se aplica.

2.4 Independência Tecnológica

Não se aplica.

3 ESTRATÉGIA PARA A CONTRATAÇÃO

3.1 Natureza do Objeto

Serviço de consultoria para implantação de um Sistema de Gestão da Segurança da Informação e Privacidade (SGSI/SGPI) no âmbito do TRE-BA e obtenção de certificação na ISO 27.001 e 27.701.

3.2 Parcelamento e Adjudicação do Objeto

Por se tratar de solução simples, que envolve apenas contratação de consultoria, não é adequada a divisão em itens para adjudicação de mais de uma empresa.

3.3 Modalidade e Tipo de Licitação

Contratação por pregão eletrônico.

3.4 Classificação e Indicação Orçamentária

Orçamento de Custeio da STI – Plano Orçamentário: SEG0 – Segurança da Informação da Justiça Eleitoral - 33903504 Consultoria em Tecnologia da Informação e comunicação.

3.5 Vigência da Prestação de Serviço

A vigência da consultoria poderá ser de 6 a 12 meses.

3.6 Equipe de Apoio à Contratação

No âmbito deste Tribunal, a equipe de apoio à contratação será composta pelos membros da equipe de planejamento.

3.7 Equipe de Gestão da Contratação

No âmbito deste Tribunal, a equipe de apoio à contratação será composta pelo Gestor do Contrato e pelos fiscais demandante, técnico e administrativo. A indicação dos fiscais e seus substitutos será feita no Formulário Padrão para Contratação de Bens e Serviços.

4 ANÁLISE DE RISCOS

Referencial para a análise de riscos:

Probabilidades: 1 – insignificante; 2 – baixa; 3 – média; 4 – alta; 5 – muito alta.

Impactos: 1 – insignificante; 2 – baixo; 3 – médio; 4 – alto; 5 – muito alto.

Matriz Probabilidade X Impacto						
		Impactos				
		1	2	3	4	5
Probabilidades	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Resultados da probabilidade X impacto:

Risco baixo: zona verde (resultados de 1 a 5);
Risco médio: zona amarela (resultados de 6 a 12);
Risco alto: zona vermelha (resultados de 15 a 25).

Risco 1: TRE/BA como pioneiro na certificação ISO 27001/27701 entre os Regionais Eleitorais		Fase: processo de contratação		
Id	Dano	Probabilidade	Impacto	Resultado
1	TSE definir um outro *framework* (CIS Controls/NIST CSF, NIST SP 800-53) [3].	3	5	15
Ações de Mitigação				
Id do Dano	Ação	Responsável		
1	Alinhar o framework do TRE-BA ao definido pelo TSE (pois a solução deverá ser única para toda a JE).	Equipe de planejamento		
2				

[3] O TSE recentemente criou uma Seção de Segurança, para uniformizar as iniciativas em SI da Justiça Eleitoral (mitigação de riscos, contratação de soluções conjuntas, etc). Há um grupo de cibersegurança composto por representantes de todos os Regionais e do próprio TSE, onde reuniões periódicas tem sido realizadas. Ainda não há definição quanto à estratégia a ser obedecida por todos os Tribunais Eleitorais.

Ações de Contingência		
Id do Dano	Ação	Responsável
1	Revisar os estudos preliminares ou o termo de referência	Equipe de planejamento

Risco 2: Licitante adjudicado não assinar o contrato		Fase: processo de contratação		
Id	Dano	Probabilidade	Impacto	Resultado
1	Não contratação da consultoria.	2	4	8
Ações de Mitigação				
Id do Dano	Ação	Responsável		
1	N/A			
Ações de Contingência				
Id do Dano	Ação	Responsável		
1	Reabrir o certame e chamar o segundo classificado	SGA		

Risco 3: Impugnação ao Edital		Fase: processo de contratação		
Id	Dano	Probabilidade	Impacto	Resultado
1	Não contratação da consultoria.	1	4	4
Ações de Mitigação				
Id do Dano	Ação	Responsável		
1	Cuidado na elaboração do TR tanto na especificação quanto nas exigências contratuais	SGA / Integrante administrativo		
Ações de Contingência				
Id do Dano	Ação	Responsável		
1	Repetir o procedimento	Equipe de planejamento da contratação		

Risco 4: Concorrência com Eleições Gerais/2022		Fase: processo de execução		
Id	Dano	Probabilidade	Impacto	Resultado
1	Atraso na execução da consultoria.	4	4	16
Ações de Mitigação				
Id do Dano	Ação		Responsável	
1	Planejamento para obter as certificações em exercícios distintos (ex: 27001 em 2022 e 27701 em 2023)		SGA / Integrante administrativo	
2	Definição de equipe de servidores do Tribunal ou terceiros dedicados para acompanhar a consultoria		SGA / STI	
Ações de Contingência				
Id do Dano	Ação		Responsável	
1	Postergar a contratação para 2023		Equipe de planejamento da contratação	

Equipe de Planejamento da Contratação Documento assinado eletronicamente via PAD		
Integrante Técnico	Integrante Demandante (Coordenador dos trabalhos)	Integrante Administrativo
RILSON BARROS DE ALMEIDA ***SEINFRA***	ANDRÉA OLIVEIRA ALMEIDA QUEIROZ ***SEAGG***	ONEÍZA MABEL CARNEIRO GUEDES ***GAB/SJU***
Salvador, 11 de março de 2022		