1 IDENTIFICAÇÃO DO PROJETO

NOME DO PROJETO	PERÍODO	ÁREA DE VINCULAÇÃO
Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados - PCGSIPD	07/2020 a 12/2021	TCE-RO

2 VINCULAÇÃO COM O PROGRAMA

2.1 Benefícios relacionados

a) Aplicabilidade da tríade basilar da segurança da informação: confidencialidade, integridade e disponibilidade das informações e dos processos críticos de informação deste Tribunal.

b) Maximização do desempenho da Instituição no quesito segurança da informação e privacidade de dados em sua estrutura organizacional.

2.2 Vinculação com o Plano de Área

a) Elaboração de uma nova Política Corporativa de Segurança da Informação (PCSI), a fim de definir um conjunto de regras, procedimentos, padrões, normas e diretrizes a serem seguidos por todos que estejam inseridos no contexto organizacional desta Corte de Contas.

b) Implantação do Programa de Conformidade à Lei Geral de Proteção de Dados Pessoais, com o objetivo de gerenciar e planejar as fases, ações, programação e controle de uma série de atividades integradas de forma a atingir o objetivo de ficar em conformidade com a Lei Geral de Proteção de Dados Pessoais.

3 PROJETOS CONEXOS, PREDECESSORES E SUCESSORES

3.1 Política de Gestão Documental – PGD, em desenvolvimento pela Comissão de Gestão Documental do TCE-RO.

4 OPORTUNIDADE / PROBLEMA

4.1 Descrição

Em ataques cibernéticos recentes, grupos de *hackers* têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos. Logo, os sistemas, as informações, as comunicações e as pessoas - o elo mais fraco da Segurança da Informação -, que integram o contexto das organizações como um todo, demandam cuidados frente às ameaças a que estão expostos, principalmente durante a pandemia, que, graças ao isolamento social, levou diversos trabalhadores, tanto do âmbito público, quanto privado, a adotarem o regime de trabalho em casa (*home office*), prática que elevou a vulnerabilidade da infraestrutura tecnológica e dos sistemas de dados de empresas e órgãos públicos.

Diante desse cenário, por meio da resolução n. 287/2019, esta Corte de Contas instituiu o Comitê de Segurança da Informação e Comunicação - COSIC, com o objetivo de estabelecer diretrizes e propor políticas, normas e procedimentos gerais relacionados à gestão informacional e do conhecimento no âmbito do TCE-RO, e, com esta, designou membros, conforme Portaria n. 424, de 28 de junho de 2019, para, assim então, estruturar os passos a serem traçados no que se refere a segurança da informação e privacidade de dados em consonância com as leis, normas e boas práticas que regem o tema.

4.2 Contextualização

A segurança da informação e privacidade de dados é um tema que envolve diferentes aspectos de organização, desde os locais onde a informação é armazenada, até os recursos humanos e tecnológicos. Abrange processos de trabalho, relação com fornecedores e prestadores de serviço, uso adequado das ferramentas e serviços de tecnologia da informação, cuidados com o ambiente de trabalho e publicação de normas que regulamentam o tema.

Com o avanço da tecnologia e dos sistemas de informações, as organizações públicas e privadas começaram a automatizar seus processos e sistemas, o que expandiu suas fronteiras para uma melhor prestação de serviços e execução de suas atividades finalísticas. Consequentemente ampliou os riscos do negócio passando a conviver com vulnerabilidades e ameaças físicas e lógicas do ambiente organizacional. Sendo assim, surgiu a necessidade de estruturar, controlar e manter seguro, não apenas o ambiente tecnológico, mas toda a organização de forma transversal.

a) **Por que esse projeto é importante para o Tribunal de Contas do Estado de Rondônia?**

Atualmente, não existe estrutura organizacional que concentre segurança da informação e privacidade de dados no Tribunal de Contas do Estado de Rondônia. Cada área, via de regra, atua dentro da sua concepção para aplicação de boas práticas de segurança e privacidade, sendo que, majoritariamente, não há integração entre elas, o que torna ainda mais complexo o tema em questão, visto que o mesmo contempla toda a organização de forma transversal e sistêmica.

No intuito de minimizar a ausência de uma estrutura centralizada de governança, segurança e privacidade de dados, esta Corte de Contas instituiu o Comitê de Segurança da Informação e Comunicação - COSIC, conforme Resolução n. 287/2019[1], com o objetivo de estabelecer diretrizes e propor políticas, normas e procedimentos gerais relacionados à gestão informacional e do conhecimento no âmbito do Tribunal de Contas de Rondônia.

b) **Quais organizações, grupos ou pessoas serão beneficiados por esse projeto e como?**

O Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados – PCGSIPD beneficiará todo o Tribunal de Contas do Estado de Rondônia, o jurisdicionado e a sociedade em geral, através da aplicação de duas frentes de atuação do projeto, quais sejam: a elaboração da nova Política Corporativa de Segurança da Informação e a implantação do Programa de Conformidade à Lei Geral de Proteção de Dados Pessoais. Deste modo, será possível buscar a garantia dos três princípios basilares que norteiam a segurança da informação, a confidencialidade, integridade e disponibilidade, em conformidade com as diretrizes da Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais – LGPD, e, com as normas da família NBR ISO/IEC 27000, para assim, maximizar o desempenho desta Corte de Contas no quesito segurança da informação, privacidade e proteção de dados em sua estrutura organizacional.

5 ESCOPO DO PROJETO

5.1 Objetivo Geral (em relação à oportunidade ou à solução do problema)

Implantar o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados - PCGSIPD, com base nas normas da família NBR ISO/IEC 27000[2], a fim de maximizar o nível de confidencialidade, integridade e disponibilidade das informações e processos críticos de informação do TCE-RO, além de adequar-se à Lei n. 13.709/2018[3] - Lei Geral de Proteção de Dados Pessoais, por meio de ações voltadas à aplicação de diretrizes, de forma a potencializar o desempenho do Tribunal nos aspectos de segurança da informação, privacidade e proteção de dados.

5.2 Descrição do Projeto

O Comitê de Segurança da Informação e Comunicação - COSIC, juntamente com o Encarregado de Proteção de Dados (*Data Protection Officer* – DPO) do TCE-RO, sugerem a implantação de um Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados - PCGSIPD, em consonância

[1] Publicada no DOe TCE-RO - nº 1893, de 26.06.2019.

[2] Conjunto de normas, em que cada uma possui uma função específica, mas todas possuem como finalidade precípua a criação, manutenção, melhoria, revisão, funcionamento e análise de um Sistema de Gestão de Segurança da Informação.

[3] Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, tendo em vista a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

com a Lei n. 13.709/2018 e com as normas ISO 27000, para, desta forma, maximizar o desempenho da Instituição no diz respeito a segurança da informação, privacidade e proteção de dados em sua estrutura organizacional.

Este programa propõe um conjunto básico de ações estruturantes que fortalecem, amparam a gestão da Segurança da Informação e Privacidade de Dados no âmbito do TCE-RO, a partir da utilização e aplicação de controles mais elevados do que os empregados atualmente, e, com estas, delineiam ações para aplicação de diretrizes de segurança da informação e de adequação à LGPD.

Ele deverá ser seguido por todos aqueles que se relacionam direta ou indiretamente com a Instituição, tais como servidores, estagiários, prestadores de serviços, parceiros e terceirizados.

O programa está estruturado em duas grandes frentes de atuação: a elaboração da nova Política Corporativa de Segurança da Informação e suas políticas inter-relacionadas e a implantação do Programa de Conformidade à Lei Geral de Proteção de Dados Pessoais, observando as leis, regulamentos, normas e boas práticas, nacionais e internacionais, que versam sobre o tema.

5.3 Produtos

Material	Entregável
Nova Política Corporativa de Segurança da Informação (PCSI)	Com a adoção de padrões, procedimentos e diretrizes da nova PCSI em conformidade com as leis, regulamentos, normas de segurança da informação, bem como a LGPD, cuja finalidade é que estas políticas sejam aprovadas pela direção, publicadas e levadas ao conhecimento do público interno.
Política de Privacidade de Dados Pessoais	
Política de *Cookies*	
Política de *Backup*	
Política de Transferência de Informação	
Política de Classificação da Informação	
Política de Gestão de Riscos e de Tratamento e Respostas a Incidentes de Segurança da Informação	
Política de *Privacy by Design* e *Privacy by Default*	
Plano de Gestão da Continuidade do Negócio	

Política de Segurança em Recursos Humanos	
Política de Controle de Acesso	
Política de Segurança Física e do Ambiente	
Política para uso de Dispositivos Móveis e Trabalho Remoto	
Política de Utilização da Internet e da Intranet e comportamento nas Redes Sociais	
Política *BYOD* - Equipamentos pessoais no ambiente corporativo	
Política de Segurança da Informação no Gerenciamento de Projetos	
Política de Gestão de Ativos	
Política para o uso de Controles Criptográficos	
Política de Segurança nas Operações	
Política de Gestão de Mudanças	
Política de Segurança nas Comunicações	
Política para Aquisição, Desenvolvimento e Manutenção de Sistemas	
Programa de Conformidade à LGPD, contendo nove itens.	Elaboração de um projeto com vistas ao planejamento e gerenciamento das fases, ações, programação e controle de uma série de atividades integradas, a fim de atingir o objetivo de ficar em conformidade com a Lei Geral de Proteção de Dados Pessoais.
Plano de Comunicação e Divulgação de Segurança da Informação	Certificar que a segurança da informação e privacidade de dados sejam partes integrantes do ambiente do TCE-RO, a fim de promover a divulgação interna de materiais sobre o tema, por meio da distribuição de cartilhas de boas práticas, manuais de conduta, políticas, dicas de segurança, informes sobre treinamentos e a criação de campanhas educativas, dentre outros.
Programa Orçamentário de Combate a Incidentes de Segurança da Informação	Propiciará investimentos específicos na segurança da informação e privacidade de dados, com a finalidade de conferir confidencialidade, integridade e disponibilidade das informações e recursos tecnológicos. Será entregue um Projeto, com o intuito de criar um programa orçamentário de segurança da informação e privacidade de dados.

5.4 Não-escopo

a) Não será incumbência deste projeto a aquisição das normas ABNT NBR ISO/IEC. É necessário que as normas façam parte do acervo do Tribunal de Contas, pois estas contribuirão para o embasamento das ações e boas práticas propostas voltadas ao aprimoramento da segurança da informação, privacidade e proteção de dados.

b) O projeto não contempla a implantação de infraestrutura, nem a aquisição de equipamentos de informática e demais acessórios. É necessário que haja infraestrutura prévia que suporte o projeto e que atenda por completo as necessidades básicas iniciais de implantação.

c) O projeto não contemplará a contratação de equipes terceirizadas para suprir as necessidades funcionais do projeto. É necessário, que, se após definidas as funções e especialidades que o TCE-RO dispões de recursos humanos para executar as atividades, elas sejam insuficientes, contrate-se profissionais com as especialidades exigidas para desempenho em cada área.

d) O projeto não ficará encarregado por organizar equipes para regular a rotina de funcionamento do projeto. É necessário que se defina por meio de estudos, as metas e padrões funcionais de avaliação e desempenho, para que a implementação do projeto atenda às expectativas e necessidades do Tribunal com o máximo aproveitamento dos recursos disponíveis e retorno dos investimentos.

e) O projeto não contempla a criação de estrutura organizacional para manter o Programa de Conformidade à LGPD. É necessário que sejam criadas estruturas e rotinas organizacionais no modelo PDCA para suportar o Programa.

f) O projeto não contempla manter revisadas e atualizadas as Políticas Corporativas de Segurança da Informação e Privacidade revisadas. É necessário que sejam criadas rotinas organizacionais para essas atividades.

5.5 Macro etapas e Produtos Intermediários

	Etapa	Entrega	Duração	Data estimada de término
a)	Nova Política Corporativa de	Conjunto de regras, procedimentos, padrões, normas e diretrizes a serem seguidos por todos que estejam inseridos no contexto organizacional, tendo em vista garantir a	11 meses	Maio/2021

	Segurança da Informação (PCSI)	confidencialidade, integridade e disponibilidade dos ativos, além de prover uma orientação e apoio da direção para o tema de acordo com os requisitos do negócio, as leis e regulamentações relevantes, as normas de segurança da informação e à LGPD.		
b)	Programa de Conformidade à LGPD	Projeto que contempla as ações necessárias para dar cumprimento à Lei Geral de Proteção de Dados Pessoais, aprovado pela direção, publicado e comunicado ao público interno. Composto por 6 fases: Conscientização e Treinamento, *Gap Analysis* (*data mapping*), Relatório de Impacto à Proteção de Dados Pessoais – RIPD, Planejamento, Implantação e Acompanhamento.	11 meses	Maio/2021
c)	Plano de Comunicação e Divulgação de Segurança da Informação	Consiste em garantir que a segurança da informação e privacidade de dados seja parte integrante do ambiente do TCE-RO, a fim de promover a divulgação interna de materiais sobre o tema, tais como cartilhas de boas práticas, manuais de conduta, políticas, dicas de segurança, informes sobre treinamentos e a criação de campanhas educativas entre outros.	7 meses	Dezembro/2021
d)	Programa Orçamentário de Combate a Incidentes de Segurança da Informação	Busca promover investimentos específicos para a área de segurança da informação e privacidade de dados, para garantir a confidencialidade, integridade e disponibilidade das informações e recursos tecnológicos.	7 meses	Dezembro/2021

5.6 **Premissas** (fatores que, para fins de planejamento, são considerados verdadeiros, reais ou certos, sem prova ou demonstração)

a)	Engajamento integral da Alta Administração do Tribunal de Contas do Estado de Rondônia em implantar o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados -PCGSIPD, para os fins de adequar-se à Lei geral de Proteção de Dados e instituir nova Política Corporativa de Segurança da Informação;

b) Instituição do Comitê de Segurança da Informação e Comunicação - COSIC, por meio da resolução n. 287/2019;

c) Nomeação do Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer* – DPO), através da portaria n. 189 de 27 de fevereiro de 2020.

d) Entrada em vigor da Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais – LGPD, em 18 de setembro de 2020, que dispõe sobre o tratamento de dados pessoais;

5.7 **Restrições** (condições internas ou externas ao projeto que afetam o seu escopo, prazo e/ou qualidade)

a) O Tribunal não dispor das normas necessárias para licenciar e orientar as atividades de Segurança da Informação, Privacidade e Proteção de Dados.

b) O Tribunal não possuir quantitativo necessário de profissionais devidamente qualificados, conforme as exigências que cada função demanda no projeto.

c) O Tribunal não ter os insumos essenciais para suprir a necessidade do projeto, tais como: equipamentos tecnológicos com as configurações mínimas exigidas pelo projeto, espaço físico para alojar a equipe que trabalhará diretamente no projeto, sistemas que atendam às necessidades informacionais durante sua execução, entre outras questões estruturais.

d) O atraso e/ou impedimentos durante as etapas de aquisições e licitações dos produtos e serviços mínimos para executar o projeto com estabilidade e eficácia.

6 CRONOGRAMA (Ações e Atividades a serem cadastradas no Módulo Gerenciador de Atividades – JIRA com responsabilidades definidas)

7 PARTES ENVOLVIDAS NO PROJETO E RESPONSABILIDADES

UNIDADES/PESSOAS ENVOLVIDAS	NÍVEL DE ENVOLVIMENTO
Secretaria Executiva da Presidência	ALTO
Gabinetes de Conselheiros	ALTO

Gabinetes de Conselheiros Substitutos	ALTO
Ministério Público de Contas	ALTO
Corregedoria	ALTO
Ouvidoria	ALTO
Escola Superior de Contas	ALTO
Secretaria de Geral de Controle externo	ALTO
Secretaria de Geral de Administração	ALTO
Secretaria de Processamento e Julgamento	ALTO
Secretaria de Planejamento e Orçamento	ALTO
Secretaria de Tecnologia da Informação e Comunicação	ALTO
Controladoria de Análise e Acompanhamento de Despesa	ALTO
Assessoria de Comunicação - ASCOM	ALTO
Encarregado de Proteção de Dados/*Data Protection Officer* (DPO)	MUITO ALTO

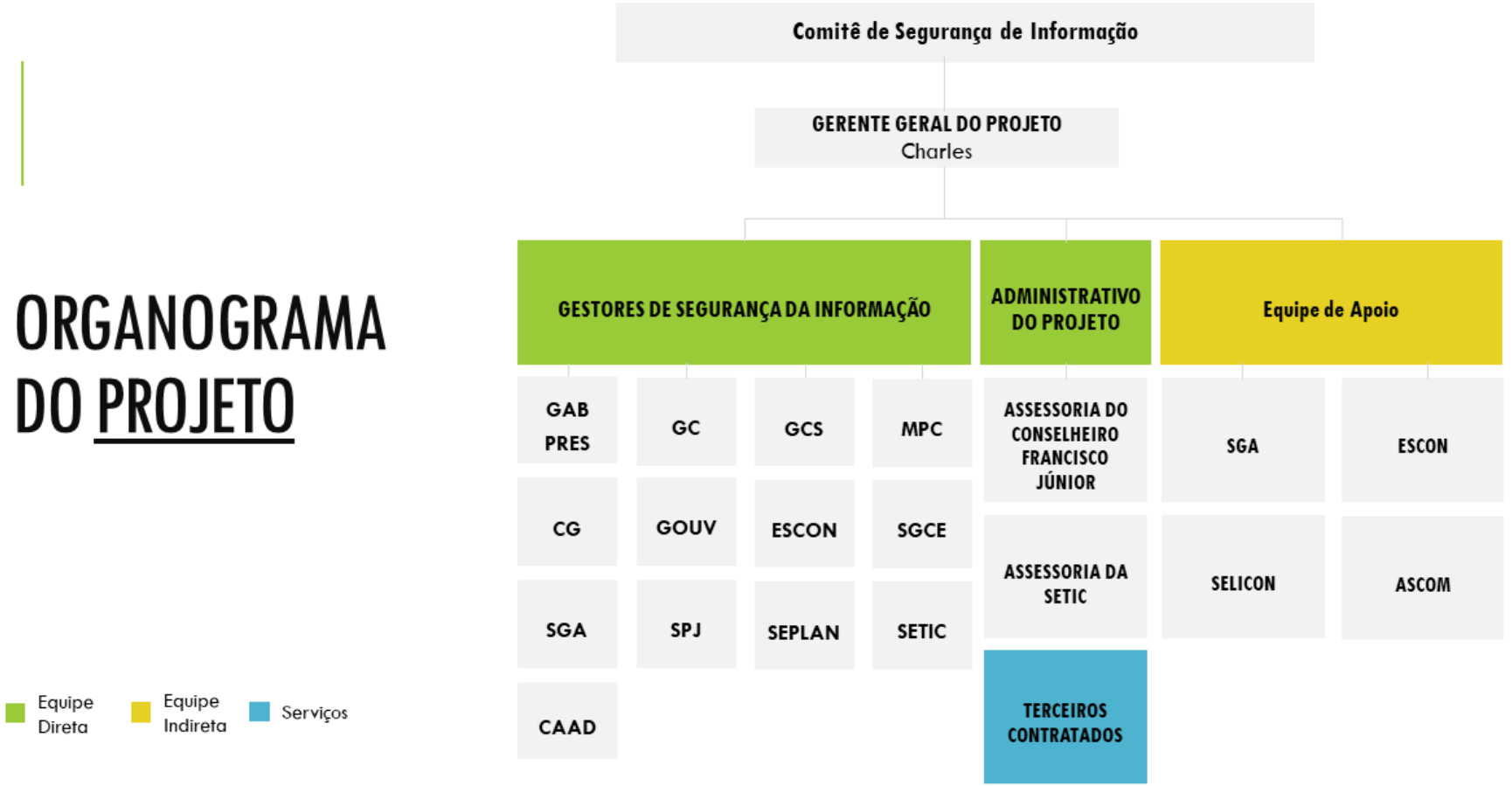
Observações:

É possível considerar que todos os setores mencionados possuem alto nível de envolvimento com o funcionamento do projeto, já que, uma vez eleito o gestor de segurança da informação e privacidade, representante de cada área, sob coordenação do DPO, serão responsáveis por disseminar, no âmbito do Tribunal de Contas do Estado de Rondônia – TCE-RO, em especial na sua área de lotação, as boas práticas sobre de segurança da informação, privacidade e proteção de dados, levar ao conhecimento da chefia e dos demais servidores as orientações institucionais relacionadas ao tema, e ainda, levar ao conhecimento do Comitê de Segurança da Informação e Comunicação (COSIC) e ao *Data Protection Officer* (DPO), ocorrências de incidentes relacionados à segurança da informação e privacidade de dados, no âmbito do TCE-RO, de que haja, mesmo que de forma indireta, tomado conhecimento. Além disso, o gestor de segurança da informação e privacidade deverá participar de capacitação e aperfeiçoamento permanente na área de segurança da informação e privacidade de dados, com foco na adequação à Lei Geral de Proteção de Dados Pessoais, e, apoiar o Comitê de Segurança da Informação e Comunicação (COSIC) e o *Data Protection Officer* (DPO) no desempenho de suas funções. Em resumo, é necessário que haja uma relação interdependente de alto engajamento entre os setores para garantir altos níveis de fluidez e eficácia na execução do projeto.

Quanto ao Encarregado de Proteção de Dados/*Data Protection Officer* (DPO), cabe a ele a coordenação das ações e atividades desenvolvidas durante e após a execução do projeto, motivo que leva tal função ao mais alto nível de envolvimento no projeto.

8 ORGANOGRAMA DO PROJETO

ORGANOGRAMA DO PROJETO



GABPRES: SECRETARIA EXECUTIVA DA PRESIDÊNCIA - GC: GABINETE DOS CONSELHEIRO - GCS: GABINETE DOS CONSELHEIROS SUBSTITUTOS - MPC: MINISTÉRIO PÚBLICO DE CONTAS - SCG: CORREGEDORIA - GOUV: OUVIDORIA - ESCON: ESCOLA SUPERIOR DE CONTAS- SGCE: SECRETARIA GERAL DE CONTROLE EXTERNO - SGA: SECRETARIA GERAL DA ADMINISTRAÇÃO - SPJ: SECRETARIA DE PLANEJAMENTO E JULGAMENTO - SEPLAN: SECRETARIA DE PLANEJAMENTO E ORÇAMENTO - SETIC: SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - CAAD/TC: CONTROLADORIA DE ANÁLISE E ACOMPANHAMENTO DE DESPESA

10 FATORES QUE PODEM COMPROMETER O PROJETO OU BENEFICIÁ-LO

OPORTUNIDADE/AMEAÇA	IMPACTO	PROBABILIDADE	(A) ACEITAR (D) DESISTIR (P) PREVENIR (R) MITIGAR	RESPONSÁVEL

Devido à sobrecarga de tarefas do time de desenvolvimento, poderá ocasionar atraso na fase 3 do projeto.	MÉDIO	MÉDIA	MITIGAR	Ainda não definido
Devido à necessidade de ajustes necessários no plano de contas, poderá ocasionar atraso na fase 3 do projeto.	MÉDIO	MÉDIA	MITIGAR	Ainda não definido
Devido à provável necessidade de adquirir equipamentos, poderá haver atrasos no início da execução do projeto.	ALTO	BAIXO	PREVENIR	Ainda não definido
Devido à provável necessidade de contratação de pessoal para suprir as necessidades funcionais do projeto, poderá haver acúmulos, atrasos e desfalques na execução do projeto.	MÉDIO	MÉDIO	PREVENIR	Ainda não definido
Devido à instabilidade das vias e métodos que compõem os processos de aquisições de bens e serviços, especialmente durante a pandemia, e que afetam diretamente as fases licitatórias, principalmente, poderá ocasionar atrasos na fase inicial de funcionamento do projeto	ALTO	MÉDIO	PREVENIR	Ainda não definido
Atraso na realização das ações para aplicação das diretrizes de Segurança da Informação e Privacidade de Dados e de adequação à LGPD nesta Corte de Contas, excedendo o no espaço de tempo estimado de 18 (dezoito) meses.	ALTO	BAIXO	PREVENIR	Ainda não definido

Aquisição tardia das normas (ABNT NBR ISO/IE) voltadas para o aprimoramento da segurança da informação e privacidade de dados nesta Corte.	ALTO	BAIXO	PREVENIR	Ainda não definido

Aprovado por:

Paulo Curi Neto

Conselheiro-Presidente do Tribunal de Contas do Estado de Rondônia

Decisão Monocrática: 0132/2021-GP