PLANO DE GESTÃO DE RISCOS DE TIC

2022

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL

Sumário

Apresentação

O Plano de Gestão de Riscos (PGR) de Tecnologia da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul foi elaborado com o intuito de incluir na rotina das equipes técnicas de TI, as principais práticas de gestão de riscos abarcadas pelos normativos utilizados como referência, quais sejam:

1. Resolução CNJ 370/2021, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
2. Norma ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes
3. Norma ABNT NBR ISO 31010:2012 - Gestão de riscos - Técnicas para o processo de avaliação de riscos
4. TCU - Referencial Básico de Gestão de Riscos
5. TCU - Manual de Gestão de Riscos
6. Resolução TRE/MS n.657/2019 - Dispõe sobre a Política de Gestão de Riscos no âmbito do TRE/MS
7. Manual de Gestão de Riscos do TRE/MS

A gestão de riscos nas organizações é um grande instrumento que auxilia no processo de tomada de decisões pelos gestores, haja vista que, ao fazer uma análise preditiva dos eventos negativos que podem ocorrer durante a execução dos planos de trabalho, consegue-se evitar eventuais consequências desfavoráveis, bem como minimizar os impactos do que não pode ser evitado, diminuindo, assim, a probabilidade de insucesso dos projetos institucionais quando da ocorrência de eventos inesperados.

Contextualização

O Plano de Gestão de Riscos (PGR) de TIC do Tribunal Regional Eleitoral de Mato Grosso do Sul foi elaborado com vistas a atender o disposto no art. 37, da Resolução CNJ n. 370/2019, abaixo colacionado:

> Art. 37. Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.

A Resolução citada alhures estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 2021-2026 e define o Índice de Serviços Críticos com Gestão de Riscos como um dos indicadores do objetivo estratégico "Aprimorar Segurança da Informação e a Gestão de Dados".

O intuito de tal exigência consiste na possibilidade de avaliar se processos considerados críticos na organização estão mapeados e se são aplicados os princípios e técnicas que norteiam a gestão de riscos na execução das rotinas de trabalho da STI.

Ademais, o Plano de Gestão de Riscos de TIC é um dos itens elencados e exigidos no questionário do iGovTIC-JUD, índice utilizado pelo Conselho Nacional de Justiça (CNJ) para identificar, avaliar e acompanhar a situação da Governança, Gestão e Infraestrutura de TIC nos órgãos do Poder Judiciário.

Processo de Gestão de Riscos

Conforme mencionado anteriormente, o presente documento teve como baluarte os princípios e definições contidos na Política de Gestão de Riscos do TRE-MS, bem como no Manual de Gestão de Riscos, ambos elaborados e revisados pela Assessoria de Governança e Projetos Institucionais deste Regional.

Em que pese os documentos citados abarcarem toda a estrutura metodológica e técnica utilizada para o mapeamento dos riscos de TIC, far-se-ia redundante estabelecer nomenclaturas e definições no presente documento.

Destarte, foi elaborada pelo Núcleo de Governança de TI, em conjunto com as coordenadorias da STI, a planilha abaixo, contendo os principais riscos operacionais, estratégicos e de integridade, relacionados à Secretaria de Tecnologia da Informação, bem como medidas de controle e de mitigação de eventuais efeitos nefastos decorrentes.

O Plano de Gestão de Riscos de TIC será administrado, avaliado e revisado periodicamente pelo Núcleo de Governança de TI, em parceria com as unidades responsáveis da Secretaria de Tecnologia da Informação do TRE-MS. com apoio metodológico e técnico da Assessoria de Governança e Projetos Institucionais - AGPI.

ANEXO I

Planilha com os riscos de TIC mapeados

Plano de Gerenciamento de Riscos de TIC

Nome do processo, projeto, plano ou programa: Elaboração do Plano de Gestão de Riscos de TIC - processo SEI 0004212-15.2022.6.12.8000					**Avaliação dos Riscos**				**IDENTIFICAÇÃO E DEFINIÇÃO DO CONTROLE EXISTENTE**	**Plano de Contingência de Riscos**	**Gestor Responsável**
Objetivo do plano: Listar os riscos de TIC, em especial aqueles associados com a continuidade do negócio											
Responsável / Gestor: Luciana Jucineire Vieira de Aguiar					**Probabilidade (vide Aba 1)**	**Impacto (vide Aba 2)**	**Valor (probabilidade x impacto)**	**Nível do Risco (Vide Aba 4)**	**Descrição do controle existente**	**O que fazer? (Antes do risco acontecer - contenção – ou depois do risco acontecer – contingência -, conforme o caso) [As ações devem combater ou explorar a causa do risco]**	
Área impac-tada	**Evento de Risco**	**Categoria do Risco**	**Causas**	**Impactos**							
STI	Interrupção de manutenções preventivas do Datacenter ou dos equipamentos da solução de backup/Rack-cofre por parte das empresas contratadas	Operacional	Falta de recurso humano, técnico ou financeiro que impeça a realização das manutenções ou apenas falta de organização	Parada do Datacenter e sistemas que estão funcionando no ambiente e/ou parada do Rack cofre e da solução de backup instalada naquele ambiente	2	10	20	14	Não há controle por parte da STI. As empresas informam que determinada data estarão realizando a manutenção preventiva e a equipe técnica acompanha. Caso não informem sobre as manutenções, não temos controle para cobrar que realizem.	Contenção: fiscalização deve estabelecer processo interno para cobrar o correto cumprimento das agendas de manutenções. Contingência: implantação do site backup no TRT24	Fiscais de contrato - Clodoaldo Fonseca e Ulysses Neto
STI	Interrupção de manutenções preventivas e corretivas do Datacenter ou dos equipamentos da solução de backup/Rack-cofre, seja por encerramento de garantia ou cobertura contratual, seja por cancelamento contratual	Operacional	Nenhum proponente interessado comparece, ou por ausência de interessados na licitação, ou em decorrência de inabilitação ou de desclassificação das propostas, no caso de licitação e rescisão contratual por parte das atuais empresas	Parada do Datacenter e sistemas que estão funcionando no ambiente e/ou parada do Rack cofre e da solução de backup instalada naquele ambiente	2	10	20	14	Monitoramento da vigência dos contratos, para iniciar processo de renovação/contratação com tempo hábil para efetuá-los antes do encerramento dos atuais.	Contenção: fiscalização deve acompanhar contrato atual para avaliar o correto cumprimento das agendas de manutenções Contingência: iniciar processo de contratação com tempo hábil para tramitação (máximo 8 meses antes) e implantação do site backup no TRT24	Fiscais de contrato - Clodoaldo Fonseca e Ulysses Neto
STI	Erro na realização dos backups ou insconsistência nas cópias de segurança	Operacional	Fita com problema; Storage cheia; erro na gravação do backup etc	Comprometimento dos dados que deveriam ser armazenados para futura recuperação e/ou falha na recuperação dos dados em função de alguma necessidade	4	10	40	18	Alertas da solução de backup sobre a execução dos backups Quanto à inconsistências nas cópias de segurança, não há controle	Contenção: SGI deve monitorar os alertas para verificar caso ocorra erros na execução dos backups. E, estabelecer processo de restauração para validar dados backupeados. Contingência: Resolver o erro e realizar novo backup.	SGI - Ulysses Almeida e Clodoaldo Fonseca
STI	Falha nos equipamentos que suportam o datacenter ou dos equipamentos da solução de backup/Rack-cofre (ar-condicionado, nobreaks, elétrica, geradores etc)	Operacional	Vida útil dos equipamentos	Parada do Datacenter e sistemas que estão funcionando no ambiente e/ou parada do Rack cofre e da solução de backup instalada naquele ambiente	4	10	40	18	Monitoramento do ambiente do Datacenter e do Rack-cofre geram alarmes e abertura de chamados no sistema de ITSM	Contenção: Manutenções preventivas. Contingência: Acionar a empresa contratada para sanar as falhas apresentadas.	SGI - Ulysses Almeida e Clodoaldo Fonseca
STI	Falha na comunicação do TRE-MS com o TSE e/ou Cartórios Eleitorais	Operacional	Rompimento de fibra ou descontinuidade do contrato	Indisponibilidade dos serviços essenciais ou não de TI para os usuários internos e externos	4	10	40	18	Monitoramento dos links de comunicação (perda de pacote, indisponibilidade etc)	Contenção: Monitoramento dos links de comunicação Contingência: Acionar a empresa contratada para sanar as falhas apresentadas.	SGI - Thiago Marinho e Robson Kobayashi
STI	Interrupção dos serviços de suporte aos usuários do TRE-MS por rotatividade de colaboradores superior à 50% da equipe em período curto de tempo	Operacional	Rotatividade alta de colaboradores terceirizados, com a falta de repasse adequado das funções a serem desempenhadas, visto que os novos integrantes não detêm a experiência da atividade.	Comprometimento das unidades da STI para dar vazão ao excessivo número de chamados que se acumularão.	2	6	12	9	Dirimir tais ocorrências mediante o acompanhamento do quantitativo de chamados abertos, pendentes de solução. E, monitorar rotatitivade de colaboradores.	Contenção: fiscalização deve acompanhar contrato e atuar para redução do índice de pendências nos chamados abertos e sem solução. Além de acompanhar a rotatividade de colaboradores. Contingência:comunicar a contratada sobre a(s) ocorrência(s) do fato e, a critério da fiscalização, exijir medidas corretivas.	Fiscais de contrato - Marcelo Novaes e Thalles Torchi
STI	Interrupção dos serviços de suporte aos usuários do TRE-MS devido à encerramento de cobertura contratual	Operacional	Atual contratado não tiver interesse em renovar, ou nenhum proponente interessado comparece, ou por ausência de interessados na licitação, ou em decorrência de inabilitação ou de desclassificação das propostas.	Interrupção da prestação de serviços de suporte aos usuários da infraestrutura de Tecnologia da Informação.	2	6	12	9	Antes do encerramento do contrato, sem possibilidade de apostilamento, demandar a criação do DOD para nova contratação.	Contenção: fiscalização deve acompanhar contrato atual e monitorar o saldo de serviços existentes. Contingência: iniciar processo de contratação com tempo hábil para tramitação (máximo 8 meses antes)	Fiscais de contrato - Gustavo Pinho, Márcio Naka, Marcelo Novaes e Thalles Torchi

STI	Interrupção no funcionamento do ITSM (GLPI)	Operacional	Falha na estrutura que suporta o sistema que possa retirá-lo do ar.	Paralisação da abertura de chamados pelos usuários e gestão dos chamados pela STI	2	6	12	9	Chamados de mal funcinamento do sistema	Contenção: Monitoramento do funcionamento pela SGS e intervenções da CODESC, caso necessário. Contingência: reinstalar a aplicação e restaurar backups do banco e filesystem.	SGS - Thalles Torchi e SBDIS - Patrícia Harumi
STI	Interrupção dos serviços de outsourcing de impressão do TRE-MS devido à encerramento de cobertura contratual	Operacional	Atual contratado não tiver interesse em renovar, ou nenhum proponente interessado comparece, ou por ausência de interessados na licitação, ou em decorrência de inabilitação ou de desclassificação das propostas.	Interrupção da prestação de serviços de outsourcing de impressão da Secretaria do TRE-MS e ZEs.	2	6	12	9	Antes do encerramento do contrato, sem possibilidade de apostilamento, demandar a criação do DOD para nova contratação.	Contenção: fiscalização deve acompanhar contrato atual e monitorar o saldo de serviços existentes. Contingência: iniciar processo de contratação com tempo hábil para tramitação (máximo 8 meses antes)	Fiscais de contrato - Márcio Naka e Ramon Rodrigues
STI	Interrupção dos serviços de manutenção preventiva de urnas eletrônicas devido à encerramento da cobertura contratual	Operacional	Falta de planejamento para realizar contratação em tempo hábil	As urnas eletrônicas deixarão de passar por ciclos periódicos de verificação, podendo resultar em número elevado de defeitos durante a preparação para as eleições	2	6	12	9	Solicitação orçamentária para contratações periódicas	Contenção: fiscalização do contato deve iniciar estudo de nova contratação ou renovação do contrato com antecedência Contingência: fazer o ciclo do STE com a equipe da Central de Atendimento	Fiscais de contrato - Domingos Sávio e Juarez Potêncio
STI	Diminuição da força de trabalho de seções da CITIS cuja área de atuação suporta processos críticos da instituição: Seção de Gestão de Infraestrutura - suporta toda a estrutura da comunicação TRExZEs e TRExTSE e a gestão de hardware e software do datacenter contêiner e esquema de cópias de segurança	Estratégico	coincidência em período de férias, licenças, mudança de lotação	diminuição / paralisação de projetos na área afetada; problemas no suporte aos processos suportados pela área	4	6	24	13	Revezamento entre os servidores de cada seção para férias e outras situações de ausência	Contenção: repassar atividades rotineiras das seções especializadas para a central de serviços de TI Contingência: com a ausência repentina de pessoal na unidade, incluir especialista no contrato de terceirização	Coordenador - Marcelo Novaes
STI	Rescisão abrupta contrato terceirização Central de Serviços	Estratégico	empresa com problemas trabalhistas/legais	alocação de servidores efetivos para realizar todo o atendimento, com consequente diminuição na quantidade de chamados atendidos	1	15	15	15	Contratação emergencial de outra empresa prestadora do serviço	Contratação emergencial de empresa	Fiscais do contrato - Thalles Torchi e Marcelo Novaes
STI	Indisponibilidade licenças/aparelhos checkpoint nas zonas e postos eleitorais	Estratégico	término prazo contratual sem nova contratação / indisponibilidade orçamentária para renovação contratação licenças	paralisação de atualizações dos aparelhos; uso da reserva técnica para suprir equipamentos com defeito	1	6	6	6	Aquisição periódica de licenças de uso	acompanhar os prazos contratuais para renovar ou iniciar outros quando necessário	Seção de Gestão de Infraestrutura - Ulysses Almeida
STI	Não recomposição da força de trabalho da COCLE de 2016, de modo que possa exercer suas atribuições regimentais relacionadas ao pleito com eficiência	Estratégico	saída de pessoal sem lotação de servidor em substituição ou remanejamento de atividades para outra unidade	falta de pessoal para realizar as atividades; no período eleitoral, necessidade de contar com apoio temporário de pessoal de outras unidades	4	3	12	8	Não há plano existente e não está listado como evento que podem impactar o alcance do objetivo estratégico pela área de pessoal. A ação concreta que existe é a formalização de um processo SEI, informando da necessidade de recomposição.	Contenção: lotar servidor com perfil para desenvolver as atividades da unidade	COCLE - Elisabete (solicitação de pessoal)
STI	Contratação tendenciosa para favorecer fornecedor específico	Integridade	Ausência de procedimentos que evitem especificações tendenciosas	Favorecimento do abuso de posição em prol de interesses privados. Violação aos princípios da Administração Pública, como a moralidade, impessoalidade e eficiência.	2	3	6	5		Adoção de política de integridade nas contratações realizar reuniões com possíveis fornecedores junto a outros representantes do órgão	responsável pela contratação
STI	reuniões restritas com possíveis fornecedores	Integridade	má fé para benefício do agente público desconhecimento de normas do código de ética	favorecimento de possível fornecedor com troca de vantagens ao agente público	2	3	6	5		Adoção de política de integridade nas contratações Realizar reuniões com possíveis fornecedores junto a outros representantes do órgão	responsável pela contratação
STI	Repasse de tais informações a terceiros	Integridade	Ausência de procedimentos que evitem acessos restritos a pessoas não autorizadas	Favorecimento a terceiros em prol de interesses privados. Violação aos princípios da Administração Pública, como a moralidade,	4	6	24	13		Atenção à legislação pertinente	responsável pela contratação
STI	Manutenção do acesso de Colaboradores desligados aos sistemas do órgão	Integridade	Ausência de procedimentos para troca de informações entre as unidades que fazem o cadastro dos colaboradores	Realização de alterações indevidas que possam prejudicar a integridade dos sistemas	4	6	24	13	supervisor da Central informa os fiscais sobre o desligamento	Seguir as boas práticas em Segurança da Informação	Fiscais do contrato - Thalles Torchi e Marcelo Novaes
STI	Subtração de ativos de TIC permanentes	Integridade	Ausência de controle de saída dos bens do órgão	Perda total ou parcial dos bens, uso indevido	2	3	6	5	normas do Núcleo de Segurança Institucional sobre entrada/saída	Uso de procedimentos para controlar a saída de bens do órgão Verificações periódicas acerca da localização dos bens de TIC	SGA - Ramon Pereira Rodrigues

STI	acesso ou concessão de acesso indevido aos dados e informações, inclusive com uso de persuasão e eventual ingenuidade dos usuários - "engenharia social".	Integridade	Ausência de cultura de segurança da informação e comunicação	Causar alterações indevidas que possam prejudicar a integridade dos dados.	2	6	12	9	acessos são dados mediante artigos da base de conhecimento do GLPI	Seguir as Boas Práticas em Segurança da Informação	CSI
STI	manipulação e alteração de dados e informações para benefício próprio ou de terceiros	Integridade	Ausência de cultura de segurança da informação e comunicação	Causar alterações indevidas que possam prejudicar a integridade dos dados.	2	6	12	9		Seguir as Boas Práticas em Segurança da Informação	CSI
STI	disponibilização de lista de eleitores com dados sensíveis	Integridade	má-fé para privilegiar 3º interessado fornecimento dos dados através de canal que não façam classificação da informação	Desrespeito à LGPD	4	6	24	13		Na esfera da unidade: fluxo de processo definido para que a solicitação do fornecimento dos dados seja feita através de sistema que permite restringir o acesso à informação (SEI), juntamente com critérios como quem é o responsável pelo pedido (Juiz Eleitoral)	SECAD - Rodrigo Baltuilhe
STI	liberação indevida de acesso ao sistema ELO	Integridade	má-fé para privilegiar 3º interessado falta de definição de política de acesso a ativos lógicos	Desrespeito à LGPD Potencial vazamento de dados	4	6	24	13	Definição de regras para a autorização de acesso ao sistema ELO, bem como revisão anual dos acessos: - ELO TRE: o cadastro de pessoas é feito com autorização da CRE - ELO ZE: acesso gerenciado por cada cartório eleitoral anualmente é encaminhada lista de usuários para CRE para providências	Contenção: Definição de regras para a autorização de acesso ao sistema ELO, bem como revisão anual dos acessos: - ELO TRE: o cadastro de pessoas é feito com autorização da CRE - ELO ZE: acesso gerenciado por cada cartório eleitoral anualmente é encaminhada lista de usuários para CRE para providências Contingência: excluir o acesso indevido assim que for identificado	SECAD - Rodrigo Baltuilhe
STI	preparação de mais de uma urna da mesma seção, manipulando a votação em urna escondida e fazendo a troca da mídia de resultado no momento da transmissão	Integridade	má-fé para privilegiar 3º interessados falta de controles e supervisão durante o período de preparação de urnas	prejuízo à lisura do processo eleitoral	1	1	1	1	Os sistemas utilizados são lacrados pelo TSE, pela tabela de correspondência onde se tem os dados das urnas que devem funcionar no dia da eleição ficam cadastrados seus códigos. Assim: 1) quando concluída a preparação das urnas na ZE, é verificada pela equipe de suporte da COCLE a lista de seções preparadas (códigos da tabela de correspondência) com a quantidade de urnas previstas para cada ZE (seção e contingência) , estando OK, vão compor o arquivo publicado na internet; 2) No dia da eleição, o sistema de totalização só aceita BUS das urnas oficiais (cujo código está na tabela de transmissão), gerando pendência caso um arquivo vindo de urna estranha a esse controle, que é resolvida pelo juiz eleitoral no momento da transmissão. *tabela de correspondência: código gerado no momento da preparação de urnas para determinada seção.	Contenção: manter os controles já existentes Contingência: na eventualidade de recebimento de BU que gere pendência em relação à correspondência, o Juiz Eleitoral deverá justificar o motivo.	COCLE - Elisabete
STI	Administração de banco de dados - uso indevido ou manipulação de dados	Integridade	falta de controle de acesso ao banco de dados	Divulgação/mal uso de informações restritas	2	3	6	5	acessoo ao banco de dados costuma ser apenas do pessoal técnico responsável	1 - Estipulação de regras de quem e o que pode acessar com as unidades envolvidas. 2 - Uso e acesso restrito de usuários com permissão DBA no banco de dados	SBDIS - Robson Rossettini