PODER JUDICIÁRIO
DO ESTADO DO ACRE

RELATÓRIO DE EXECUÇÃO DE GESTÃO DE RISCO DE TI **2021-2026**

PERÍODO 07/2024 A 03/2025

Diretoria de Tecnologia da Informação
ditec@tjac.jus.br

1. Introdução

Este relatório apresenta uma visão consolidada dos riscos identificados na área de TI, conforme registrado na planilha “Consolidação – Processo de Gestão de Riscos Simplificado”. Ele visa auxiliar a alta gestão e as equipes operacionais na compreensão dos principais riscos—seus causadores, consequências, controles já implementados e as respectivas respostas estratégicas. Com base nessa análise, serão apontadas recomendações e próximos passos para o fortalecimento da resiliência operacional e da segurança dos ativos de TI.

2. Escopo e Objetivos

Escopo:
Levantamento e análise dos riscos relacionados à infraestrutura, segurança, continuidade dos serviços, governança e gestão dos recursos humanos em TI, considerando tanto aspectos preventivos quanto contingenciais.

Objetivos:

Identificar e descrever os eventos de risco, suas causas e consequências, avaliando os níveis de risco inerente (antes dos controles) e o risco residual (após os controles aplicados), mapeando os controles preventivos e contingenciais existentes sugerindo ações de mitigação, melhoria ou reorganização dos processos para reduzir vulnerabilidades, estabelecendo um processo contínuo de monitoramento e comunicação dos riscos.

3. Metodologia e Critérios de Análise

Para a avaliação dos riscos, foram considerados os seguintes elementos, conforme os dados apresentados na planilha:

Identificação dos Eventos: Cada risco é identificado por um ID e descrito por meio do “Evento de Risco”, acompanhado de suas Causas e Consequências.

Avaliação Quantitativa e Qualitativa:

Probabilidade: Classificada, por exemplo, em “1: MUITO BAIXA”, “2: BAIXA”, “3: MÉDIA” e “4: ALTA”.

Impacto: Definido por valores numéricos e descrições (ex.: “RELEVANTE”, “MUITO RELEVANTE”, “EXTREMO”) que mensuram a gravidade do efeito de cada risco.

Nível de Risco Inerente (NRI): Combinação da probabilidade com o impacto antes da aplicação dos controles.

Fator de Controle (FC): Indicador da eficácia dos controles existentes que atuam na prevenção e na mitigação dos riscos.

Nível de Risco Residual: Risco remanescente após a implementação dos controles, que serve de base para a definição da resposta estratégica.

Resposta e Ações mitigadoras:

Cada evento possui uma estratégia de resposta (como “MITIGAR/MELHORAR” ou “EVITAR/EXPLORAR”) e ações específicas, com responsáveis e prazos definidos, que são essenciais para reduzir ou eliminar o risco.

4. Sumário dos Riscos – Principais Eventos Identificados

A planilha apresenta uma série de eventos agrupados em categorias. Abaixo, esta exemplificado alguns riscos representativos:

ID	Evento de Risco	Probabilidade	Impacto	NRI	Nível de Risco Residual	Resposta
1	Acesso não autorizado	2: BAIXA	4: MUITO RELEVANTE	8	3.2 (Alto)	MITIGAR/MELHORAR
3	Acidente no manuseio de equipamentos/abastecimento do tanque	1: MUITO BAIXA	4: MUITO RELEVANTE	4	3.2 (Médio)	EVITAR/EXPLORAR
4	Tempestades atmosféricas e oscilações elétricas	3: MÉDIA	4: MUITO RELEVANTE	12	7.2 (Alto)	EVITAR/EXPLORAR
5	Cópia de segurança dos dados não disponíveis ou comprometida	2: BAIXA	5: EXTREMO	10	6 (Mediano)	MITIGAR/MELHORAR
...	...	...	...	...	...	...

Nota: A tabela resume os principais indicadores de alguns eventos selecionados para exemplificar a estrutura adotada na análise.

5. Análises Detalhadas dos Principais Riscos por gerencias

GESER

ID	RISCO	CATEGORIA	IMPACTO	PROBABILIDADE	VALOR	CRITICIDADE	AÇÃO
1	Cabeamento lógico com falhas	Operacional/Infraestrutura	4	2	8	Alto	Revisar e modernizar o cabeamento, priorizar recursos para upgrade
2	Ausência de política de segurança em sala segura	Compliance/Segurança	4	5	20	Alto	Formalizar e implantar política de segurança, com controles de acesso e monitoramento
3	Goteiras na cobertura prejudicando equipamentos	Operacional/Patrimônio	5	3	15	Alto	Realizar manutenção urgente na cobertura e realocar equipamentos sensíveis
4	Terceirização sem supervisão eficaz	Estratégico/Contratual	4	3	12	Médio	Fortalecer monitoramento dos contratos e treinamentos das equipes terceirizadas
5	Indisponibilidade de serviços críticos (PJe, SAJ)	Operacional/Serviço	5	3	15	Alto	Implementar redundância e plano de contingência (PCN)

GESIS (Sistemas)

ID	RISCO	CATEGORIA	IMPACTO	PROBABILIDADE	VALOR	CRITICIDADE	AÇÃO
1	Falha em sistemas judiciais em horários críticos	Operacional	5	3	15	Alto	Monitoramento proativo/contrato de suporte 24x7
2	Desenvolvimento sem homologação adequada	Compliance/Qualidade	4	2	8	Médio	Reforçar checklist de homologação e validação de requisitos
3	Dependência de poucos analistas de sistemas	Estratégico/Recursos	4	4	16	Alto	Plano de capacitação/contratação e transferência de conhecimento
4	LGPD não implementada em todos os sistemas	Compliance	5	3	15	Alto	Revisar sistemas quanto à LGPD, adequar fluxos de dados, treinar equipe

GEGOV (Governança)

ID	RISCO	CATEGORIA	IMPACTO	PROBABILIDADE	VALOR	CRITICIDADE	AÇÃO
1	Planos e políticas não alinhados ao CNJ/IGOVTIC	Compliance/Institucional	4	3	12	Médio	Reunir com áreas, revisar documentos e ajustar normas rotineiramente
2	Falha no monitoramento do cumprimento das políticas	Estratégico	3	3	9	Médio	Auditoria interna regular/periódica e cronograma de revisão
3	Resistência a mudanças ou baixa capacitação dos servidores	Humano/Organizacional	3	4	12	Médio	Plano de treinamento contínuo e comunicação interna

Contratações (DITEC e Gestão de Pessoas)

ID	RISCO	CATEGORIA	IMPACTO	PROBABILIDADE	VALOR	CRITICIDADE	AÇÃO
1	Empresas terceirizadas não entregam níveis de serviço	Contratual/Serviço	4	3	12	Médio	Reforçar fiscalização de SLA e reuniões de acompanhamento
2	Quadro próprio insuficiente para atender a demanda	Estratégico/Recursos	5	4	20	Alto	Reforçar plano de concurso e contratação
3	Não conformidade nas contratações de TI (Res. 370)	Compliance	4	2	8	Médio	Revisar fluxos de compras, checklists jurídicos e controles internos

Tratamento dos riscos

Causas	Riscos	Tratamento
Descumprimento da política de segurança Descumprimento de normas de confidencialidade	Acesso não autorizado	• Em fase de elaboração das novas políticas de segurança. • Existem uma política vigente que está em operação. • Verificar no G2Tic ou falar com o Gestor • Risco monitorado pelo CGSIS; • Até momento não foi detectado qualquer vazamento de informações sigilosas; • Ações de mitigação à serem adotadas com capacitação dos usuários e gestores.
Equipe reduzida Excesso de atividades e demandas diárias Pouca observância aos manuais de processos Pouco conhecimento por parte de integrantes da equipe em elaboração e gerenciamento de planejamento; Ferramenta tecnológica de monitoramento sem utilização de todas funcionalidades Sistema de monitoramento e avaliação do planejamento não utilizado de forma adequada	Ineficiência de acompanhar e mensurar resultados das ações estratégicas.	• Monitorar o quadro efetivo previsto na Resolução com o quadro atual incluindo o último concurso. • Risco plenamente mitigado
Falha humana relacionada ao manuseio do grupo gerador de energia secundária.	Acidente ao manusear equipamentos ou abastecimento do tanque de combustível.	• Risco eliminado após completa readequação. • Foi isolado a área do tanque e contratado novo Data Center que atende as normas vigentes. • Risco plenamente mitigado
Acesso físico não autorizado (indevido) a sala de equipamentos de rede.	Falhas dos controles de acesso físico ao Data Center.	• Foram implementadas novas fechaduras eletrônicas. • Existe controle de acesso gerenciado; • Está sendo elaborado um protocolo de acesso a nova política de segurança;

Interrupção de energia elétrica.	Fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 horas.	● Qual a autonomia do grupo gerador com tanque cheio? ● Feita a aquisição de novo grupo gerador toando o sistema redundante; ● Existe contrato de manutenção garantindo a continuidade de serviço; ● Existe controle de combustível; ● Existe controle de validade da bateria; ● Existe controle de redundância com nobreak e com manutenção contratada.
Falhas ou queima de componentes eletrônicos.	Tempestades Atmosféricas. Oscilações Elétricas	● Solicitar a GEINS relatório sobre a efetividade da malha de aterramento do data center bem como do SPDA ● Existe aterramento certificado da sala segura.
Oscilações ou quedas na comunicação de dados entre as comarcas	Interrupção da comunicação de internet. Interrupção de fornecimento de energia. Oscilações de Energia. Falha humana.	● Solicitar a GESEG Relatório das Oscilações/Quedas de Energia. ● Risco mitigado com a contratação da Starlink com 35 unidades, garantindo redundância; ● Realizado nova contratação de fornecedora de links de fibra; ● Realizado a contração de Firewalls para as comarcas para automatizar a alternância dos links em eventual queda. ● Realizar diagnóstico de aterramento e SPDA em todas as unidades jurisdicionais, bem como relatório de análise de eficiência dos sistemas existentes. ● Fazer a aferição da qualidade da energia em todas as instalações prediais do PJAC, inclusive checar o atendimento as
Indisponibilidade de backups de dados.	Cópia de segurança dos dados não disponível ou sem integridade em razão de indisponibilidade de rede, quedas ou oscilações de energia ou erros de configuração das estratégias de backups.	● Eliminado com a contratação da Starlink, conforme descrito anteriormente.

Falhas na restauração de dados.	Erros de rede. Quedas ou oscilações de energia. Erros de configuração das estratégias de backups.	● Mudança na estratégia de backup, virtualizando. Assim, possibilitando o restore completo e mais rápido e eficiente. ● Revisão do Cabeamento Estruturado com Certificação. ● Criar e institucionalizar Política de Procedimentos e Relatórios de Incidentes dos Passivos de Rede(cabeamentos horizontal, vertical, line cords, patch cords, conectores, etc...);
Indisponibilidade de link de internet redundante.	Inexistência de contrato de prestação de serviços de internet para link backup.	● Eliminado com a contratação da Starlink, conforme descrito anteriormente.
Bloqueio ou dificuldades de acesso físico as unidades jurisdicionais	Alagamento. Desabamento. Incêndio. Infiltrações decorrentes de águas da chuva e ventanias após evento de destelhamento. Problemas decorrentes de vazamento de água potável, Drenos dos equipamentos condensadores de ar condicionado entupidos, causando inundação no piso elevado ou em cima dos equipamentos. Inundação causada por evento de chuvas que podem comprometer sistemas pluviais internos de escoamento de águas.	● Fazer um checklist de diagnóstico detalhado dos riscos por comarca. Ex: Alagamento, ● Incidente ocorrido na Comarca de Xapuri onde a caixa d´água está instalada sobre a sala do servidor; ● Providenciar relatório quanto a existência do mesmo fenômeno nas demais comarcas do interior.
Equipamentos de climatização da sala do data center com mau funcionamento	Variação de temperatura na sala segura	● Eliminado com a contratação de empresa especializada em climatização de Data Centers.
Falhas no acesso ao Storage de dados	Indisponibilidade de rede de comunicação de dados. Oscilações de energia elétrica. Procedimento incorreto de acesso ao Storage. Procedimento incorreto de configuração do Storage.	● Eliminado conforme as ações adotadas nos riscos anteriores correlacionados.
Falha ou indisponibilidade do sistema unificado de autenticação de usuários	Procedimento incorreto no sistema de autenticação unificado. Indisponibilidade de rede de comunicação de dados. Oscilações ou quedas de energia elétrica.	● Eliminado conforme as ações adotadas nos riscos anteriores correlacionados.

falta de restruturação dos equipamentos e cabos da rede estruturada (logica, telefônica e elétrica), substituição dos cabeamentos lógicos em todas as unidades do poder judiciário, Dificuldades em adquirir novos equipamentos, necessidade de garantir recursos para modernização dos sistema de cabeamento em todas as unidades do TJAC	Erros de configuração de ativos de rede. Queda ou oscilações de energia elétrica. Queima ou falhas de componentes eletrônicos. Falta de conhecimento sobre manutenção preventiva e corretiva em cabeamento estruturado. Ausência de capacitações em redes de comunicação de dados.	● Recomendar checklist de diagnóstico situacional por unidade. ● Os ativos de rede estão cobertos pela garantia e backups. ● Mitigado com a substituição do sistema de telefonia convencional para o Sistema VOIP; ● Nas comarcas do interior, foi feito o upgrade da categoria dos cabos lógicos da 5 para a 6. Possibilitando assim o aumento da velocidade da conexão e renovação com cabeamento estruturado.
Falhas ou erros no acesso à sistema ou banco de dados.	Inexistência de conectividade de rede. Falhas ou erros na configuração do serviço. Comprometimento do sistema operacional. Ataques internos e externos	● Mitigado com segmentação e restrição dos acessos. ● Será eliminado com a aquisição de ferramenta PAM.
Atraso na implantação do Pje, aquisição de nova sala cofre, capacitação de servidores para atuar na implementação.	Ausência de equipamentos para hospedagem do sistemas, necessidade de capacitação de servidores, falta de contratação de empresa fabrica de software	● Data Center adquirido e todas as exigências necessárias foram implementadas com capacitações, contratações e aquisições.
Inexistência de políticas de valorização	Servidores sem políticas de valorização, servidores desmotivado,	● Adequar a redação da Causa
Falha no controle de patrimônio	Perda de etiqueta de patrimônio, falta de cadastro no GRP referente ao número de série do equipamento, remanejamento sem autorização da DITEC, extravio de equipamentos durante a fase pandemia	● Está sendo elaborado um estudo para implantação de uso do sistema de RFID, que possibilitará a substituição das etiquetas de tombo atuais. ● Haverá a coleta de dados para um novo inventário geral de todos os equipamentos de TIC.
Indisponibilidade parque tecnológico compatível com a demanda, Inexistência de políticas de substituição de equipamentos por tempo de uso	hardware obsoleto, incompatibilidades com sistemas, aumento da demanda de serviços,	● Elaborar política de substituição do parque tecnológico. ● Atualmente, 90% do parque tecnológico foi renovado; ● Política de renovação do parque com prazo máximo definido.(Verificar resolução CNJ);
Inexistência de controle de mudanças de equipamentos de locais	Dificuldades com planejamento sobre os patrimônios ativos	● Elaborar política de mudança de equipamentos.

		• Definir normatização, procedimentos, Treinamentos e Conscientização a nível institucional com relação a movimentação dos equipamentos de TIC.
Alta demanda de reparos de impressoras, contratar empresa de outsourcing de impressão	ineficiência para atender demanda de impressão	• Reunir com Diretoria e avaliar ações • A Atual Gestão do PJAC adotou a política de impressão "zero"; • Realizar estudo para definir as unidades e subsidiar a criação de uma política de impressão e inovação tecnológica de transformação digital.
Falta de controle sobre as tomadas estabilizadas falhas de energia elétrica, Inexistência de aterramento adequado nos edifícios, problemas em nobreak	Indefinição da fiscalização sobre usabilidade	• Elaborar checklist das causas possíveis e encaminhar para a engenharia para providências. • Não existe etiquetas de identificação nas tomadas; • Falta de política de controle de uso das tomadas; • Tomadas fora da conformidade com as Normas Técnicas NBR 5410; • Realizar reunião com os stakeholders.
Deficiência em melhorar os resultados do Índice de Governança de Tecnologia da Informação e Comunicação (iGovTIC-JUD)	Perda da capacidade de planejar, dificuldades de definir métricas	• Melhorar os relatórios, Implementar metodologia de acompanhamento e aferição dos indicadores
Falta de divulgação dos resultados do iGovTIC-JUD	Criticidade alta pela falta de recursos humano, capacitação, valorização, possibilidade altíssima de não cumprimentos dos macros desafios do planejamento estratégico, deficiências na elaboração, monitoramento e execução dos planos previstos na resolução 370 CNJ, dificuldades que comprometem a implementação de sistemas estruturantes da PDPJ, com Pje, e sistemas satélites.	• Divulgação está sendo realizada via portal G2TI e conect jus
Impossibilidade de Constituir e manter estruturas organizacionais privilegiando a departamentalização por função e possuindo níveis hierárquicos de decisão	Incapacidade de continuidade dos serviços	• Restruturação das Unidades

Deficiência em manter a estrutura organizacional, o quadro permanente de servidores, a gestão de ativos e os processos de gestão de trabalho da área de TIC do órgão adequados às melhores práticas para as atividades consideradas como estratégicas	Perda da capacidade de planejar, dificuldades de definir métricas, falta de central de serviços, governança e gestão de TIC, inexistência da implantação da resolução 236/2019	● Falta de Macroprocessos na distribuição de demandas afeta o controle de prazo das entregas; ● Criação de um fluxo de análise de viabilidade, priorização, execução e suporte.
Não manter a coordenação dos macroprocessos de TIC e as funções gerenciais executadas preferencialmente por servidores do quadro permanente do órgão	Falta de central de serviços, governança e gestão de TIC, inexistência da implantação da resolução 236/2019	● Analisar a referida resolução e ver o que já feito. ● O mesmo que se aplica ao item anterior.
Inexistência de ações que promove à retenção de talentos de TIC	Evasão de profissionais especializados para outros setores internos, outros órgãos e empresas privada.	● Adoção de políticas de valorização implementadas com investimentos em infraestrutura, capacitação e valorização financeira.
Inexistência de análise de rotatividade de servidores de TIC	Evasão de profissionais especializados para outros setores internos, outros órgãos e empresas privada.	● Relatório produzido e disponibilizado no G2T
Deixar de alinhar o Planos Diretores de Tecnologia da Informação e Comunicação (PDTIC) à Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)	Não cumprimento da resolução e macros desafios da planejamento estratégico	● Planos alinhados
Deixar de acompanhar os resultados das metas institucionais e nacionais estabelecidas.	Não cumprimento da resolução e macros desafios da planejamento estratégico, ausência de ferramentas de gestão	● Metas acompanhadas através dos planos, BI portal g2tic
Não Elaborar propostas orçamentárias alinhadas ao PDTIC	Falta de cumprimento de metas e ações dos planos estratégicos, falta da mensuração dos desenvolvimentos	● Proposta orçamentárias elaboradas em conjuntos com a DIGES

Deixar de realizar contratação de serviços de desenvolvimento e de sustentação de sistemas de informação obedecendo os requisitos estabelecidos na ENTICJUD	criticidade alta pela falta de recursos humano, capacitação, valorização, possibilidade altíssima de não cumprimentos dos macros desafios do planejamento estratégico, deficiências na elaboração, monitoramento e execução dos planos previstos na resolução 370 CNJ, dificuldades que comprometem a implementação de sistemas estruturantes da PDPJ, com PJe, e sistemas satélites.	● Risco mitigado com a realização de concurso público e reposição de servidores do quadro. ● Foi realizado a contratação de empresa fabrica de software
Disponibilizar junto ao repositório nacional artefatos de contratações	Não cumprimento da resolução e macros desafios da planejamento estratégico, ausência de ferramentas de gestão	● Risco mitigado, todos os artefatos estão sendo publicado
Deixar de fomentar a aderência dos processos de aquisições de bens e contratação de serviços de TIC às determinações do CNJ	Falta de capacitação, falta de investimentos, inexistência da implantação da resolução 236/2019	
Inexistência de adoção de padrão nacional definido pelo CNJ para a utilização das credenciais de login único e interface de interação dos sistemas	Não cumprimento da resolução e macros desafios da planejamento estratégico, falta de ferramenta de integração de software.	● Foi mitigado com a integração do SAJ ao PDPJ e de alguns sistemas administrativos ao Market place do TJAC. ● Pendente de autorização da Alta Gestão para o uso do PDPJ como via única de Login.
Não manter a gestão dos ativos de infraestrutura tecnológica	Dificuldade para manter o funcionamento operacional do parque computacional tornando indisponível todos os sistemas judiciais, administrativos e extrajudicial.	● A GESEG possui gerenciamento de gestão de seus ativos através da ferramenta open source NetBox, Possui ainda uma ferramenta opensource de monitoramento de funcionamento online dos ativos ZABBIX fornecendo relatórios automáticos real time.
Interrupção de energia elétrica.	Fator interno que comprometa a rede elétrica do prédio com curto circuitos, incêndios e infiltrações.	● Solicitar de emissão de Laudo Técnico pela Engenharia
Vulnerabilidade da sala segura	Falta de proteção externa a sala segura	● Atualmente é mitigado com instalações de câmeras de vigilância;

		• A Sala Segura possui controle de temperatura, partículas, incêndios e alagamento monitorado com alarme.
		• Será contemplado na nova política de segurança.

5.1. Riscos Relacionados à Segurança da Informação

5.1.1. Acesso Não Autorizado (ID 1)

Causas:
Descumprimento das políticas de segurança e das normas de confidencialidade.

Consequências:
Vazamento de informações sigilosas, sequestro de dados e potenciais danos à imagem institucional.

Controles existentes:

Políticas de segurança já em vigor (com revisão em andamento), monitoramento pelo CGESI e ações de capacitação dos usuários.

Avaliação:
Probabilidade baixa (2: BAIXA), impacto considerado muito relevante (4: MUITO RELEVANTE) resultando em um NRI de 8; o risco residual é reduzido para 3.2.

Recomendações:
Atualizar as políticas de segurança, intensificar a capacitação dos usuários e reforçar a vigilância contínua junto à alta gestão.

5.2. Riscos na Disponibilidade da Infraestrutura

5.2.1. Acidente no Manuseio dos Equipamentos/Abastecimento do Tanque (ID 3)

Causas:
Falha humana no manuseio do grupo gerador de energia.

Consequências:
Interrupção no fornecimento de energia para o Data Center, afetando diretamente a continuidade dos serviços.

Controles Implementados:
Isolamento da área de risco, contratação de um novo Data Center com conformidade às normas vigentes.

Avaliação:
Probabilidade muito baixa (1: MUITO BAIXA) com impacto muito relevante, resultando em NRI de 4 e risco residual de 3.2.

Recomendações:
Realizar treinamentos específicos para operações críticas e revisar periodicamente os procedimentos para manuseio e abastecimento.

5.3. Riscos Decorrentes de Fatores Externos

5.3.1. Tempestades Atmosféricas e Oscilações Elétricas (ID 6)

Causas:
Condições climáticas adversas levando à queima de componentes eletrônicos ou oscilações.

Consequências:
Indisponibilidade de serviços, perda de informações e interrupção dos recursos críticos.

Controles Implementados:
Aterramento certificado da sala segura e realização de análises periódicas dos sistemas de proteção (SPDA).

Avaliação:
Probabilidade média (3: MÉDIA) e impacto muito relevante (4: MUITO RELEVANTE), resultando em NRI de 12 e risco residual elevado de 7.2.

Recomendações:
Reforçar a manutenção preventiva dos sistemas de aterramento e SPDA, acompanhando a eficiência desses controles por meio de relatórios e auditorias regulares.

5.4. Riscos Relacionados à Integridade dos Dados

5.4.1. Falhas nas Cópias de Segurança (ID 8)

Causas:
Problemas de conectividade, oscilações de energia ou configurações inadequadas nas estratégias de backup.

Consequências:
Risco de perda irreversível de dados e dificuldade na recuperação dos sistemas, comprometendo a continuidade do negócio.

Controles Implementados:
Processos de backup diários e monitoramento dos volumes de dados.

Avaliação:
Probabilidade baixa (2: BAIXA) e impacto extremo (5: EXTREMO), com NRI de 10 e risco residual de 6.

Recomendações:
Investir em novas tecnologias de backup e revisar periodicamente as configurações de backup para garantir a integridade e disponibilidade dos dados.

5.5. Riscos relacionados à Governança e Recursos Humanos

Diversos eventos na planilha apontam para desafios na capacidade de acompanhamento dos resultados, na retenção e capacitação de profissionais de TI.

Exemplo:

Identificado nos eventos com IDs 18 e 19, onde a falta de ações para a valorização e retenção dos profissionais de TIC pode comprometer o desempenho estratégico e operacional.

Consequências:
Rotatividade elevada, acúmulo de demandas e dificuldade na execução dos planos estratégicos.

Recomendações:
Estruturar programas de capacitação contínua, desenvolver planos de valorização e implementar métricas de acompanhamento da rotatividade e desempenho da equipe.

6. Segurança da Informação

Risco 1: Acesso Não Autorizado

Causas: Falhas nas políticas de segurança e confidencialidade.

Consequências: Vazamento de informações sensíveis e risco de sequestro de dados.

Controles: Troca periódica de senhas.

Mitigações Propostas: Treinamento em segurança de dados e novas ferramentas de gestão.

Risco 13: Falhas no Acesso ao Storage

Causas: Procedimentos incorretos e oscilações na rede.

Consequências: Indisponibilidade de sistemas e dados.

Controles: Políticas de acesso e uso de storages redundantes.

Mitigações Propostas: Monitoramento diário e replicação de dados.

7. Continuidade de Serviços

Risco 4: Interrupção de Energia Elétrica

Causas: Fatores externos que afetam a rede elétrica.

Consequências: Paradas nos serviços TI.

Controles: Geradores de energia e manutenção.

Mitigações Propostas: Capacitar equipes para ações de contingência.

Risco 6: Oscilações de Energia e Comunicação

Causas: Falhas humanas e instabilidade energética.

Consequências: Indisponibilidade de recursos.

Controles: Relatórios de eventos.

Mitigações Propostas: Estreita comunicação com concessionária de energia.

8. Gestão de Ativos e Patrimônio

Risco 19: Falha no Controle de Patrimônio

Causas: Perda de identificação de patrimônio e registros.

Consequências: Dificuldade no planejamento e controle.

Controles: Conferências e uso de checklist.

Mitigações Propostas: Implementação de sistema de gestão de ativos mais robusto.

Risco 21: Planejamento de Patrimônio Ativo

Causas: Mudanças não controladas no inventário.

Consequências: Equipamentos não monitorados corretamente.

Controles: Diagnóstico situacional.

Mitigações Propostas: Metodologia de controle aprimorada.

9. Capacitação e Motivação da Equipe

Risco 18: Desmotivação da Equipe

Causas: Falta de políticas de valorização.

Consequências: Alta rotatividade.

Controles: Inexistentes.

Mitigações Propostas: Desenvolvimento de planos de valorização.

Risco 29: **Evasão de Talentos**

Causas: Ausência de retenção de profissionais.

Consequências: Sobrecarga de trabalho.

Controles: Adoção de metodologias motivacionais.

Mitigações Propostas: Compensação financeira e reconhecimento.

10. Planejamento Estratégico

Risco 25: Incumprimento da Resolução CNJ

Causas: Falta de recursos humanos e capacitação.

Consequências: Falhas na implementação de sistemas.

Controles: Divulgações e acompanhamento.

Mitigações Propostas: Programas de treinamento e monitoramento mais eficaz.

Risco 31: Alinhamento de Planos Diretores

Causas: Falha no planejamento estratégico nacional.

Consequências: Ineficiências operacionais.

Controles: Monitoramento das metas.

Mitigações Propostas: Alinhamento e revisão constante dos planos.

11. Principais Desafios e Oportunidades

Desafios

Efetividade dos Controles:

Alguns riscos ainda apresentam níveis residuais elevados, indicando que os controles existentes precisam ser aprimorados ou repensados.

Infraestrutura e Conectividade:

Dependência de ativos físicos e de fornecimento de energia, que podem ser impactados por fatores externos (ex.: tempestades e oscilações elétricas).

Governança e Gestão de Pessoas:

Gaps na capacitação e na retenção de talentos podem comprometer a execução efetiva dos planos de ação estratégicos.

Oportunidades

Atualização das Políticas e Processos:

Revisão e unificação das políticas de segurança e dos procedimentos operacionais para aumentar a aderência e a eficácia dos controles.

Investimento em Tecnologia:

Adoção de novas ferramentas de monitoramento, backup, e gestão de ativos reduziu os riscos operacionais significativamente.

Melhoria na Governança:

Implantar uma rotina de monitoramento dos indicadores de risco (NRI e risco residual) e promover a comunicação efetiva com a alta gestão, possibilitando respostas ágeis e assertivas.

12. Recomendações Estratégicas

Fortalecimento dos Controles de Segurança:

Revisar as políticas de acesso e aprimorar os sistemas de monitoramento e gestão de acessos, minimizando riscos de intrusão e vazamento de informações.

Melhoria da Infraestrutura:

Implementar e monitorar planos preventivos para manutenção dos sistemas elétricos (ati-SPDA, aterramento, redundância de energia), bem como aprimorar as soluções de backup, a fim de garantir a recuperação integral dos dados.

Capacitação e Retenção de Talentos:

Desenvolver programas de treinamento contínuo e planos de valorização para reduzir a evasão de profissionais especializados, garantindo uma equipe bem preparada e alinhada aos desafios estratégicos.

Monitoramento e Revisão contínua:

Estabelecer ciclos de revisão periódica dos indicadores de risco, conforme as frequências previstas (diária, mensal, semestral ou bimestral), e adotar relatórios de acompanhamento para apoiar a tomada de decisão da alta gestão.

Monitoramento Regular

- implementar medidas corretivas onde necessário.
- **Método:** Uso de relatórios situacionais para avaliar o progresso e garantir que os controles preventivos e contingenciais estejam funcionando eficazmente.
- **Responsáveis:** Gestores de risco das unidades envolvidas (DITEC, GESEG, entre outros).

Capacitação Contínua da Equipe

- **Descrição:** Promover treinamentos regulares com foco em ferramentas de monitoramento e gestão de riscos.
- **Objetivo:** Garantir que a equipe técnica tenha conhecimento atualizado sobre melhores práticas de monitoramento.
- **Responsáveis:** Diretores de equipe com suporte da ESJUD.

Implementação de Indicadores

- **Descrição:** Desenvolver e acompanhar indicadores de desempenho relacionados à mitigação dos riscos identificados.
- **Objetivo:** Mensurar com precisão os impactos das ações preventivas e determinar áreas que requerem maior atenção.
- **Responsáveis:** Gerentes de segurança e diretores da DITEC.

Relatórios Frequentes

- **Descrição:** Elaborar relatórios mensais, bimestrais ou semestrais com análise detalhada do status de cada ação planejada e dos riscos monitorados.
- **Objetivo:** Comunicar os resultados e permitir que todas as partes interessadas estejam alinhadas com os avanços do plano.
- **Responsáveis:** Gerente responsável pelo plano estratégico e pelo monitoramento do progresso.

Revisão e Ajustes estratégicos

- **Descrição:** Reavaliar periodicamente os controles e as estratégias implementadas para garantir a adequação às necessidades de TI e aos objetivos do TJAC.
- **Objetivo:** Identificar lacunas ou oportunidades de melhoria e ajustar os planos de resposta aos riscos.
- **Responsáveis:** Alta gestão da DITEC e presidência.

Adoção de Ferramentas Avançadas

- **Descrição:** Planejar e adquirir sistemas automáticos de monitoramento que permitam maior eficiência e abrangência na gestão dos riscos.
- **Objetivo:** Substituir processos manuais por soluções tecnológicas modernas, reduzindo erros e aumentando a confiabilidade do monitoramento.
- **Responsáveis:** Diretoria da DITEC.

Comunicação Efetiva

- **Descrição:** Estabelecer um plano de comunicação claro para relatar progressos, desafios e ações pendentes às equipes internas e externas.
- **Objetivo:** Manter transparência e colaboração em todas as fases do monitoramento.
- **Responsáveis:** Diretores de setor e gerentes de riscos.

Controle Sobre Infraestrutura

- **Descrição:** Garantir que os ativos de TI sejam monitorados continuamente, com substituição de equipamentos obsoletos e ações corretivas em caso de falhas.
- **Objetivo:** Mitigar riscos operacionais e garantir a continuidade dos serviços.
- **Responsáveis:** Diretores da DITEC e gestores patrimoniais.

Planejamento para Longo Prazo

- **Descrição:** Propor iniciativas que garantam a sustentabilidade do plano de monitoramento, incluindo a alocação de recursos orçamentários e humanos adequados.
- **Objetivo:** Assegurar a continuidade e evolução do progresso nas estratégias de mitigação de riscos.
- **Responsáveis:** Presidência e alta gestão do TJAC.

13. Conclusão

A análise dos riscos de TI, fundamentada nos dados da planilha "Consolidação – Processo de Gestão de Riscos Simplificado", revela um cenário diversificado que abrange desde aspectos de segurança da informação e infraestrutura até desafios de governança e gestão de pessoas. Apesar dos diversos controles já implementados, alguns riscos apresentam níveis residuais significativos, ressaltando a necessidade de ações contínuas de melhoria e monitoramento.

A implementação das recomendações estratégicas apresentadas neste relatório—em especial, a atualização dos controles, o investimento em tecnologia de backup e a capacitação dos profissionais—garantirá uma postura mais resiliente e proativa frente aos riscos, assegurando a continuidade dos serviços críticos para a organização.

- **Implementação dos Planos de Ação:**
  Definir cronogramas e responsabilidades para a execução das ações recomendadas.
- **Revisões Periódicas:**
  Atualizar os indicadores de risco e os relatórios de monitoramento de acordo com as frequências estipuladas na planilha para garantir a evolução dos controles e ações de mitigação.
- **Comunicação com a Alta Gestão:**
  Manter fluxo contínuo de informações por meio de relatórios e reuniões periódicas, assegurando o suporte estratégico necessário para a implementação dos ajustes.

Este documento consolida os dados apresentados na planilha, proporcionando uma visão abrangente dos riscos, suas causas, os controles existentes e as ações estratégicas necessárias para mitigar os impactos na operação de TI. Caso seja necessário aprofundar algum aspecto específico ou integrar gráficos e análises complementares, este relatório poderá ser expandido conforme a evolução da gestão de riscos.