PLANO DE GESTÃO DE RISCOS DE TIC
– 2026 –

PODER JUDICIÁRIO
DO ESTADO DA BAHIA

Apresentação

Este documento apresenta os resultados das atividades de tratamento dos riscos que foram identificados, analisados e avaliados no Plano de Gestão de Riscos da SETIM para o período de 2025/2026 em conformidade com modelos, resoluções e normas em geral relativas ao assunto, em especial atendendo às diretrizes definidas pelo CNJ.

A partir das definições deste documento, os principais riscos tecnológicos receberam plano de ação para tratamento dos riscos de TIC conforme definições da Política de Gestão de Riscos e do Manual de Gestão de Riscos da SETIM, este documento foi elaborado conforme previsto na Ordem de Serviço TJBA-36/21-S e OS G1-149-Sprint 005, que tratam do plano de tratamento do Plano de Gestão dos Riscos 2025/2026.

Tribunal de Justiça do Estado da Bahia

5ª Avenida do CAB, 560 – Salvador-BA – Brasil

www.tjba.jus.br

Histórico de revisões

Data	Versão	Descrição
25/09/2022	1.0	Versão inicial
18/03/2026	1.1	Versão 1ª revisão

Sumário

1 Introdução

A Secretaria de Tecnologia da Informação e Modernização (SETIM) do Tribunal de Justiça do Estado da Bahia (TJBA), comprometida com a consolidação de uma governança de TIC robusta, eficiente e orientada a resultados, elaborou o Plano de Tratamento de Riscos de Tecnologia da Informação e Comunicação para o ciclo 2025/2026. Este plano complementa o esforço institucional dedicado à identificação, análise e avaliação dos riscos tecnológicos, traduzindo-os agora em ações concretas, priorizadas e alinhadas às diretrizes estratégicas do Tribunal e às recomendações dos órgãos reguladores, em especial o Conselho Nacional de Justiça (CNJ).

A etapa de tratamento de riscos constitui um marco fundamental na evolução do processo de gestão de riscos da SETIM, pois representa a transição da análise conceitual para a execução estruturada de medidas destinadas a reduzir as vulnerabilidades, mitigar ameaças e fortalecer a resiliência dos serviços de TIC. Durante as reuniões realizadas com as coordenações da SETIM, com a Governança de TIC e com os representantes estruturantes da Secretaria, ficou evidente que a clareza sobre quais riscos serão tratados, por quem, com que prioridade e por meio de qual estratégia de resposta é indispensável para garantir consistência, transparência e efetividade dos resultados.

O trabalho desenvolvido evidenciou, ainda, que parte dos desafios enfrentados historicamente decorre da heterogeneidade na forma de registrar, descrever e classificar os riscos – incluindo dificuldades recorrentes na distinção entre risco, causa e impacto, e entre riscos estratégicos, táticos e operacionais. Assim, o Plano de Tratamento de Riscos adota rigorosamente o modelo conceitual orientado pelos referenciais ABNT NBR ISO 31000, COSO ERM, RISK IT da ISACA e pelas normas e recomendações do CNJ, estruturando cada risco a partir da relação entre Ativo de TIC, Vulnerabilidade, Ameaça e Impacto, de modo a assegurar padronização, comparabilidade e clareza.

Como premissas para o tratamento dos riscos identificados na primeira versão do Plano de Gestão de Riscos da SETIM 2025/2026, destacam-se:

- Priorização orientada ao alinhamento estratégico, assegurando que os riscos tratados sejam coerentes com o Plano de Transformação Digital (PTD), com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e com as demandas institucionais mais críticas do TJBA.
- Definição explícita da estratégia de tratamento (mitigar, evitar, transferir ou aceitar), vinculando cada risco a ações específicas, responsáveis, prazos, indicadores de acompanhamento e critérios de validação.
- Integração com práticas de governança e controles internos, garantindo aderência às auditorias, conformidade regulatória e monitoramento contínuo dos riscos residuais.
- Segregação clara de papéis e responsabilidades, preservando a independência na avaliação, na execução das ações de tratamento e na verificação da efetividade dos controles.
- Foco em riscos transversais e estruturantes, especialmente aqueles relacionados à continuidade dos serviços de TIC, à execução dos processos

críticos (como gestão de incidentes e mudanças), ao alinhamento entre ferramentas ITSM e fluxos documentados, e à manutenção de artefatos de governança.

Com essas diretrizes, o Plano de Tratamento de Riscos de TIC da SETIM busca assegurar uma atuação integrada, realista e orientada à redução consistente das exposições tecnológicas, contribuindo diretamente para a proteção dos ativos de TIC, para a estabilidade dos serviços e para o cumprimento das expectativas regulatórias do CNJ no tocante à governança, risco e conformidade.

A adoção desse modelo fortalece a maturidade institucional da SETIM e reforça o compromisso do TJBA com a transparência, a confiabilidade e a continuidade das atividades judiciais que dependem de tecnologia.

2 Plano de Tratamento dos Riscos

2.1 Apresentação do Plano

O Planejamento do Tratamento dos Riscos da SETIM para o ciclo 2025/2026 foi desenvolvido com foco em transformar a análise de riscos realizada pelas coordenações em ações práticas, priorizadas e alinhadas às diretrizes estratégicas do TJBA.

O trabalho foi construído de forma colaborativa com todas as diretorias envolvidas, garantindo visão integrada dos principais riscos que impactam a continuidade, a segurança e a eficiência dos serviços de TIC.

Esse planejamento estabelece como cada risco será tratado, definindo responsáveis, prazos, estratégias (mitigar, evitar, transferir ou aceitar) e indicadores de acompanhamento. A estrutura adotada segue os referenciais da ABNT NBR ISO 31000 e as normas do CNJ, assegurando padronização, rastreabilidade e conformidade regulatória.

Com este planejamento, a SETIM avança para um modelo mais estruturado, transparente e orientado a resultados, assegurando que o tratamento dos riscos contribua diretamente para a estabilidade e evolução dos serviços tecnológicos que sustentam as atividades do Tribunal.

2.2 Plano de Tratamento dos Riscos da Diretoria de Governança e Transformação Digital (DGT):

A Diretoria de Governança e Transformação Digital (DGT) desempenha papel estruturante na governança corporativa de TIC do TJBA. Ela responde diretamente pela manutenção de alinhamento estratégico, pelo planejamento de TIC, pela maturidade dos processos, pela monitoria das decisões estratégicas e pela capacitação digital das equipes.

Como órgão estratégico, a DGT sustenta o pilar de governança que habilita as demais diretorias a operar de forma eficiente, integrada e alinhada ao PTD e ao PDTIC.

Os principais riscos estratégicos desta diretoria se concentram majoritariamente em:

- Continuidade e estabilidade dos instrumentos de planejamento (PTD e PDTIC)
- Conformidade regulatória baseada em padrões de maturidade
- Monitoria sistemática das decisões estratégicas de TIC
- Capacitação digital de servidores e líderes

O conjunto desses riscos reflete áreas críticas para a confiabilidade institucional: governança, integração, disciplina de processos e desenvolvimento de competências necessárias à transformação digital.

O plano a seguir apresenta o tratamento de cada risco de forma executiva, orientada a resultados, com linguagem acessível aos gestores de negócio, mas preservando rigor metodológico para coordenações técnicas.

2.2.1 Risco: R01 – ID: DGT-01 - Descontinuidade dos Planos e Políticas de TIC

Tipo: Risco Estratégico

O risco representa a possibilidade de desalinhamento estratégico, interrupção de iniciativas e instabilidade na gestão do portfólio institucional, causada por mudanças frequentes de liderança, que afetam a continuidade do PTD e do PDTIC, fator que compromete a previsibilidade, governança e priorização das entregas.

Tipo de Tratamento do Risco (NRR): Controles Detectivos e Corretivos

Plano de Tratamento:

1. Definir e publicar Política de Planejamento Estratégico de TIC que estabelece diretrizes obrigatórias para revisão e revalidação do PTD e PDTIC sempre que ocorram mudanças de liderança ou alteração nos objetivos estratégicos do TJBA.
2. Criar Indicador Corporativo de Execução dos Planos (PTD/PDTIC) que permite acompanhamento institucional do avanço, aderência e maturidade dos planos.
3. Padronizar ciclos de atualização dos documentos estratégicos que garante regularidade e consistência nas atualizações, evitando paralisia ou obsolescência.
4. Instituir governança específica para validação de alterações nos planos que reduz o impacto de decisões isoladas e reforça o alinhamento institucional.

Como cada ação interfere na mitigação do risco:

1. Política de Planejamento: cria um marco normativo que impede a descontinuidade por mudanças de liderança, impondo disciplina de processo.
2. Indicador Corporativo: transforma o planejamento em objeto de gestão contínua, permitindo identificar desvios antes que gerem impacto estratégico.
3. Ciclos Padronizados: trazem previsibilidade e evitam lapsos temporais em que documentos se tornam desatualizados.
4. Governança Estruturada: protege os planos contra intervenções ad hoc, garantindo alinhamento ao nível diretivo.

Responsável pelo Tratamento: DGT / CGTIC

Situação Atual: Não iniciado

KRI: % de iniciativas PTD/PDTIC executadas ou em execução no mês.

- **Interpretação:** Esse indicador mede risco de descontinuidade estratégica e quanto menor a execução, maior o risco de desalinhamento e interrupção de políticas que viabilizam a estratégia.
- **Fórmula:** (Iniciativas em execução ou concluídas / Total de iniciativas) × 100
- **Meta:** ≥ 85%

2.2.2 Risco: R02 - ID: DGT-02 - Não Conformidade Regulatória dos Processos de TIC

Tipo: Risco Estratégico

A desigualdade no nível de maturidade dos processos de TIC gera risco de apontamentos de auditoria, falhas de conformidade, e impacto na capacidade da SETIM de se alinhar às exigências do PDTIC, iGovTIC e demais normas nacionais.

Tipo de Tratamento (NRR): Controles Detectivos e Corretivos

Plano de Tratamento:

1. Definir nível objetivo de maturidade para todos os processos de TIC
2. Implantar metodologia de avaliação periódica de maturidade
3. Criar instrumentos de fiscalização da aderência
4. Ajustar processos cujo nível esteja inferior ao padrão institucional

Como cada ação interfere na mitigação

1. Nível objetivo: estabelece norte institucional e elimina assimetrias entre processos.
2. Avaliações periódicas: permitem detectar brechas de conformidade e riscos regulatórios de forma imediata.
3. Fiscalização: reduz risco de processos operarem abaixo do compliance exigido.
4. Ajustes estruturais: garantem evolução contínua e sustentabilidade do modelo.

Responsável: DGT / CGTIC

Situação: Não iniciado

KRI: % de processos avaliados quanto ao nível de maturidade no mês

- **Interpretação:** baixa avaliação indica risco de inconformidade e fragilização do modelo de governança
- **Fórmula:** (Processos avaliados / Total de processos) × 100
- **Meta:** 100%

2.2.3 Risco:R03 – ID:DGT-03 - Desvios e Inconsistências na Monitoria das Decisões Estratégicas

Tipo: Risco Estratégico

Este risco está associado à fragmentação dos dados de monitoramento e à ausência de verificação sistemática de aderência do processo decisório aos documentos PTD e PDTIC. Isso aumenta a chance de estouros de orçamento, desalinhamento organizacional e desperdício de recursos.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento:

1. Criar indicadores de aderência às decisões estratégicas (PTD/PDTIC)
2. Implementar rotina formal de reporte ao Comitê de Governança
3. Estabelecer trilhas de responsabilização em caso de decisões não aderentes
4. Implantar painel corporativo de alinhamento estratégico das decisões

Impacto de cada ação na mitigação:

1. Indicadores de aderência: quantificam o desvio e permitem correção imediata.
2. Reporte ao comitê: eleva o nível de transparência e força disciplina organizacional.
3. Trilhas de responsabilização: reduzem decisões isoladas, estimulando conformidade.
4. Painel corporativo: reduz fragmentação de dados e aumenta governança informacional.

Responsável: DGT / CGTIC

Situação: Não iniciado

KRI: % de decisões estratégicas aderentes no mês

- **Interpretação:** Mede o risco de desvios, inconsistências e desalinhamento organizacional
- **Fórmula:** (Decisões aderentes / Total avaliadas) × 100
- **Meta:** ≥ 95%

2.2.4 Risco: R04 – ID:DGT-04 - Déficit de Competências Digitais e Baixa Aderência à Capacitação

Tipo de Risco: Estratégico

O risco decorre da baixa adesão de servidores e líderes às trilhas de capacitação, levando a falhas operacionais, baixa exploração tecnológica e dificuldade de adoção de novas soluções digitais.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Definir indicador institucional de participação em capacitação
2. Instituir trilha obrigatória de capacitação digital por perfil de usuário
3. Implementar mecanismo de convocação institucional para capacitações essenciais
4. Monitorar evolução individual e por unidade, promovendo incentivos de adesão

Como cada ação reduz o risco

1. Indicador institucional: quantifica lacunas e direciona ações corretivas.
2. Trilha obrigatória: padroniza o mínimo necessário de competência digital.
3. Convocações formais: elevam o comprometimento e eliminam adesões voluntárias insuficientes.
4. Monitoramento por unidade: cria competição saudável e aumenta engajamento.

Responsável: DGT / CGTIC

Situação: Planejado

KRI: % de servidores que concluíram trilha obrigatória no mês

- **Interpretação:** Indica risco de déficit de competências digitais e baixa capacidade de adoção tecnológica
- **Fórmula:** (Servidores capacitados / Total) × 100
- **Meta:** ≥ 95%

2.3 Plano de Tratamento dos Riscos da Coordenação de Governança de Tecnologia da Informação e Comunicações (CGTIC):

A CGTIC atua como núcleo normativo da governança de TIC da SETIM/TJBA, garantindo aderência institucional a políticas, normas, frameworks e controles, assegurando a coerência entre processos, tecnologia e requisitos de conformidade regulatória.

Os riscos desta coordenação refletem fragilidades estruturais em conformidade, governança, documentação, maturidade de processos, gestão de dados e controle de ativos.

Principais riscos mapeados:

- Reincidência de falhas por monitoramento insuficiente de riscos e controles.
- Perda de conhecimento institucional por não aderência a documentos reguladores.
- Inconsistência e falhas operacionais em ITSM/ITIL por baixa aderência técnica.
- Vulnerabilidade jurídica e reputacional no uso não supervisionado de IA.
- Exposição a vazamentos devido à ausência de inventário e governança de dados.
- Perdas de patrimônio e uso indevido de ativos por controles insuficientes.

2.3.1 Risco: R05 – ID: CGTIC-01 – Recorrência de falhas, procrastinação e reincidência em registros de riscos e controles de TIC

Tipo de Risco: Tático

Falhas e reincidências decorrem de monitoramento insuficiente, controles parcialmente implantados e registros inconsistentes, aumentando risco de apontamentos regulatórios e perda de credibilidade institucional.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Estabelecer indicadores corporativos de nível de risco de TIC.
2. Medir e acompanhar situação dos controles existentes.
3. Criar processo cíclico de atualização de controles e planos de ação

Como cada ação reduz o risco

1. Indicadores corporativos revelam falhas reincidentes.
2. Monitoria contínua evita retorno de vulnerabilidades.
3. Atualização de controles fortalece governança preventiva.

Responsável: CGTIC

Situação: Não Iniciado

KRI: % de controles e planos de ação monitorados e atualizados por mês.

Interpretação do KRI: Mede a disciplina de execução da governança de riscos. Quanto menor o percentual, maior a chance de reincidências, falhas repetidas e vulnerabilidades não tratadas.

Fórmula: (Controles/planos atualizados ÷ Total de controles/planos) × 100
Meta: ≥ 90%

2.3.2 Risco: R06 – ID: CGTIC-02 – Turnover, desconhecimento e não aderência a documentos reguladores de TIC

Tipo do Risco: Operacional

A perda de conhecimento institucional e descumprimento de normas decorrem da não adesão a políticas, normas e manuais, agravada por turnover e afastamentos, provocando degradação de processos e atrasos.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Implantar inspeções de conformidade.
2. Medir frequência de acesso aos documentos.
3. Garantir atualização anual dos documentos reguladores.
4. Registrar ciência formal dos servidores

Como cada ação reduz o risco

1. Inspeções previnem divergências práticas.
2. Monitoramento de acesso identifica lacunas de conhecimento.
3. Atualizações anuais reduzem risco de decisões baseadas em informações obsoletas.
4. Ciência formal reforça responsabilidade institucional.

Responsável: CGTIC

Situação: Não Iniciado

KRI: % de documentos reguladores atualizados e com ciência registrada por mês.

Interpretação do KRI: Indica o nível de aderência institucional às políticas e normas. Percentual baixo representa risco direto de perda de conhecimento, inconsistências operacionais e falhas de governança.

Fórmula: (Documentos atualizados e com ciência ÷ Total de documentos reguladores) × 100

Meta: 100%

2.3.3 Risco: R07 – ID: CGTIC-03 – Inconformidades nos processos ITSM por baixa aderência técnica e insuficiência de recursos.

Tipo do Risco: Operacional

Falhas nos processos ITSM surgem pela ausência de verificação de aderência, insuficiência técnica e desalinhamento ao ITIL, comprometendo qualidade dos serviços, prazos e metas.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Monitorar aderência entre ferramenta ITSM × processo mapeado × ITIL V4.

2. Definir e divulgar KPIs ITSM.
3. Publicar indicadores de aderência.
4. Alocar especialistas em governança ITSM

Como cada ação reduz o risco

1. Monitoramento de aderência reduz falhas sistêmicas.
2. KPIs evidenciam problemas e orientam ações corretivas.
3. Indicadores publicados fortalecem governança.
4. Reforço técnico reduz erros por desconhecimento.

Responsável: CGTIC

Situação: Não Iniciado

KRI: % de processos ITSM aderentes ao processo mapeado e ao ITIL por mês.

Interpretação do KRI: Percentual baixo aponta falhas de padronização, retrabalho, inconsistências e risco de degradação dos serviços. Permite verificar se a TI está de fato operando segundo melhores práticas.

Fórmula: (Processos aderentes ÷ Total de processos ITSM avaliados) × 100

Meta: ≥ 95%

2.3.4 Risco: R08 – ID: CGTIC-04 – Inconformidade legal, abusos ou violações no uso de IA

Tipo do Risco: Operacional

A falta de supervisão da aplicação de IA expõe o TJBA a abusos, violações legais, danos reputacionais e sanções regulatórias, segundo a Resolução CNJ 615.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Criar matriz RACI da governança de IA.
2. Fiscalizar aderência à Política de IA da SETIM.
3. Monitorar indicadores de conformidade no uso de IA.
4. Alocar recursos especializados em IA responsável.

Como cada ação reduz o risco

1. A matriz RACI evita usos indevidos.
2. Fiscalização previne violações legais.
3. Indicadores permitem ação rápida.
4. Recursos técnicos garantem supervisão contínua.

Responsável: CGTIC

Situação: Planejado

KRI: % de usos de IA avaliados quanto à conformidade por mês.

Interpretação do KRI: Percentual baixo indica risco elevado de uso irregular de IA, mau funcionamento, vieses, descumprimento regulatório e potencial responsabilização institucional.

Fórmula: (Usos de IA avaliados ÷ Total de usos de IA identificados) × 100

Meta: 100%

2.3.5 Risco: R09 – ID: CGTIC-05 – Vazamentos, inconsistências e uso indevido de dados digitais.

Tipo do Risco: Operacional

A ausência da governança e do inventário de dados, há risco de vazamentos, inconsistências, acessos indevidos e sanções LGPD, afetando continuidade e imagem institucional.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Executar processo estruturado de Governança de Dados.
2. Criar indicadores de percentual de dados mapeados.
3. Alocar equipe técnica de dados.

Como cada ação reduz o risco

1. Mapeamento reduz riscos de exposição.
2. Indicadores aumentam capacidade de identificar falhas.
3. Equipe dedicada acelera maturidade dos processos.

Responsável: CGTIC

Situação: Não Iniciado

KRI: % de dados digitais mapeados e inventariados por mês.

Interpretação do KRI: Valores baixos indicam risco significativo de exposição indevida, inconsistências e falhas de conformidade com a LGPD. Representa o grau de maturidade da gestão de dados.

Fórmula: (Dados mapeados ÷ Total de dados digitais identificados) × 100

Meta: ≥ 90%

2.3.6 Risco: R10 – ID: CGTIC-06 – Falhas, perdas e uso indevido de ativos de TIC por insuficiência de controle.

Tipo do Risco: Operacional

Ativos de TIC podem sofrer perdas, depredação, uso indevido ou falhas por falta de recursos técnicos, ausência de monitoramento e descentralização da gestão.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Alocar recursos técnicos para gestão de ativos.
2. Realizar verificações e monitoramento constante.
3. Criar Política de Governança de Ativos.
4. Definir indicadores de maturidade e aderência.

Como cada ação reduz o risco

1. Monitoramento reduz perdas.
2. Política padroniza responsabilidades.
3. Indicadores revelam falhas e priorizam ações.

Responsável: CGTIC

Situação: Não Iniciado

KRI: % de ativos registrados e monitorados no inventário institucional por mês.

Interpretação do KRI: Valores menores que a meta indica um risco elevado de perdas de patrimônio, uso indevido e falhas por ausência de controle centralizado.

Fórmula: (Ativos registrados e monitorados ÷ Total de ativos) × 100

Meta: ≥ 95%

2.4 Plano de Tratamento dos Riscos da Coordenação de Planejamento e Projetos de Tecnologia da Informação e Comunicações (CPTIC):

A CPTIC é responsável pelo planejamento, priorização, gestão, modelagem e monitoramento do portfólio de projetos de TIC do TJBA.

Sua atuação garante que os projetos estejam alinhados ao PTD, PDTIC e às capacidades reais de entrega da SETIM, evitando desperdícios, desalinhamentos e retrabalho.

Os riscos mapeados para a CPTIC demonstram vulnerabilidades relacionadas a gestão de portfólio, planejamento de projetos, balanceamento de demandas, conhecimento técnico das equipes e governança de processos de TIC.

Principais riscos mapeados:

- Desalinhamento estratégico e inconsistência do portfólio por falta de critérios de priorização.
- Falhas, interrupções e baixa qualidade de entregas por insuficiência de conhecimento técnico e recursos.
- Má execução e manipulação indevida do portfólio por planejamento inadequado, priorização incorreta e excesso de demandas simultâneas.
- Perda de conhecimento organizacional e execução não padronizada devido a mapas de processos desatualizados ou não utilizados.

2.4.1 Risco: R12 – ID: CPTIC-01 – Pressões setoriais e internas, perda de foco, inconsistências e desalinhamento do portfólio por falta de critérios de priorização e integração com PTD/PDTIC

Tipo de Risco: Tático

O portfólio de projetos pode tornar-se inconsistente, desalinhado e consumindo recursos de forma inadequada quando não existem critérios formais de priorização, resultando em desperdício, atrasos, incoerência com PDTIC/PTD e consumo exagerado de esforço operacional.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Formalizar critérios de priorização alinhados ao PTD e PDTIC.
2. Implantar processo estruturado de gestão de portfólio com revisões periódicas.
3. Definir limites de capacidade (WIP – Work in Progress).
4. Integrar indicadores aos relatórios gerenciais.
5. Capacitar equipes em gestão de portfólio.

Como cada ação reduz o risco

1. Critérios formais → eliminam decisões baseadas em pressões.
2. Gestão estruturada → aumenta previsibilidade e consistência.
3. Limites WIP → evitam sobrecarga e interrupções.
4. Indicadores gerenciais → promovem transparência e governança.
5. Capacitação → melhora maturidade da equipe.

Responsável: CPTIC

Situação: Planejado

KRI: % de projetos priorizados conforme critérios formais por mês.

Interpretação do KRI: KRI indica o grau de aderência do portfólio aos critérios técnicos e estratégicos. Percentual baixo significa risco de desperdício, desalinhamento e inconsistências graves no portfólio.

Fórmula: (Projetos priorizados conforme critérios ÷ Total de projetos do portfólio) × 100

Meta: ≥ 90%

2.4.2 Risco: R13 – ID: CPTIC-02 – Interrupções e falhas no portfólio por falta de conhecimento técnico e escassez de recursos

Tipo de Risco: Operacional

A insuficiência de conhecimento técnico e escassez de recursos provoca erros, omissões, interrupções e frustrações nas entregas de projetos, reduzindo a qualidade e aumentando retrabalho e insatisfação.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Implementar programa contínuo de capacitação técnica.
2. Definir matriz de competências e ajustar alocação de recursos.
3. Padronizar checklists de qualidade.
4. Implantar quality gates.
5. Registrar lições aprendidas e incentivar reuso.
6. Reforçar equipe ou priorizar demandas conforme capacidade real.

Como cada ação reduz o risco

1. Capacitação reduz erros técnicos.
2. Matriz de competências melhora alocação.
3. Quality gates padronizam qualidade e reduzem falhas.
4. Lições aprendidas evitam repetição de erros.
5. Reforço de equipe adequa capacidade à demanda.

Responsável: CPTIC

Situação: Planejado

KRI: % de entregas aprovadas nos quality gates por mês.

Interpretação do KRI: Indica maturidade e qualidade do processo de gestão de projetos. Baixa aprovação revela falhas técnicas, falta de padronização ou insuficiência de conhecimento.

Fórmula: (Entregas aprovadas ÷ Total de entregas avaliadas) × 100

Meta: ≥ 95%

2.4.3 Risco: R14 – ID: CPTIC-03 – Ações inadequadas, manipulações e interrupções por planejamento incorreto e excesso de demandas

Tipo de Risco: Operacional

O planejamento inadequado, excesso de demanda e priorização incorreta levam à má execução dos projetos, causando atrasos, interrupções, problemas técnicos e frustrações nas áreas demandantes.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Revisar e formalizar metodologia de planejamento.
2. Integrar critérios táticos ao planejamento operacional.
3. Implantar gestão de capacidade (limitar projetos simultâneos).
4. Criar comitê de replanejamento e priorização recorrente.
5. Registrar riscos de projeto e planos de resposta.

Como cada ação reduz o risco

1. Metodologia revisada → reduz erros de planejamento.
2. Critérios táticos → aumentam coerência.
3. Limite de capacidade → evita sobrecarga.
4. Comitê periódico → corrige desvios rapidamente.
5. Registro de riscos → melhora resiliência dos projetos.

Responsável: CPTIC

Situação: Planejado

KRI: % de projetos planejados com critérios de priorização e WIP aplicados por mês.

Interpretação do KRI: Mostra o grau de aderência do planejamento às boas práticas de capacidade e priorização. Níveis baixos representam risco direto de interrupções e má execução.

Fórmula: (Projetos planejados com critérios + WIP ÷ Total de projetos planejados) × 100

Meta: ≥ 90%

2.4.4 Risco: R15 – ID: CPTIC-04 – Desconhecimento, descumprimento e inconformidade de processos por mapas desatualizados ou não utilizados

Tipo de Risco: Operacional

A falta de uso e atualização dos mapas de processos leva à perda de conhecimento organizacional, atrasos, retrabalho e má execução dos serviços e projetos relacionados a TIC.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Implantar política e procedimento de gestão de processos.
2. Criar ciclo de revisão periódica dos mapas.
3. Aumentar a divulgação dos processos em portal único.
4. Realizar treinamentos e campanhas de uso.
5. Definir donos de processo.
6. Criar indicadores de uso e atualização.

Como cada ação reduz o risco

1. Política → institucionaliza a governança de processos.
2. Revisões periódicas → mantêm processos atualizados.
3. Divulgação e treinamento → ampliam uso e aderência.
4. Donos de processo → garantem responsabilidade contínua.

Responsável: CPTIC

Situação: Não Iniciado

KRI: % de processos de TIC com mapas atualizados e utilizados por mês.

Interpretação do KRI: Indica o nível de maturidade processual da coordenação. Baixa aderência significa perda de conhecimento, retrabalho e risco de execução desconexa.

Fórmula: (Processos com mapas atualizados e em uso ÷ Total de processos mapeados) × 100

Meta: ≥ 95%

2.5 Plano de Tratamento dos Riscos da Coordenação de Promoções, Contratações e Gestão de Serviços de TIC (CPROM/CCTIC):

A CPROM - Coordenação de Promoções/Contratações de TIC, também conhecida institucionalmente como CCTIC - Coordenação de Contratações de TIC é responsável por planejar, fiscalizar, organizar e monitorar o ciclo de contratações de TIC, garantindo que os serviços terceirizados, contratos estratégicos, insumos e fornecedores operem em conformidade com o PTD, PDTIC, legislação aplicável e requisitos de continuidade.

Os riscos mapeados revelam fragilidades em planejamento de contratações, aderência regulatória, controle de termos de referência, monitoramento de fornecedores, gestão documental, inventários contratuais, e cumprimento de etapas formais.

Principais riscos mapeados:

- Atrasos licitatórios e interrupções de serviços críticos por planejamento insuficiente ou desalinhado.
- Erros e impugnações de Termos de Referência causados por desconhecimento técnico ou falta de revisão.
- Ilegalidades ou vícios por treinamento insuficiente nas normas de contratação.
- Ausência de controle das etapas formais do processo de contratação resultando em atrasos e retrabalho.
- Dispersão documental e ausência de inventário centralizado de serviços terceirizados e contratos de TIC.

2.5.1 Risco: R16 – ID: CPROM-01 – Atrasos licitatórios, descontinuidade e indisponibilidade de serviços por planejamento insuficiente das contratações

Tipo de Risco: Tático

A ausência de planejamento completo das contratações de TIC, alinhado ao PTD e PDTIC, pode gerar expiração de contratos críticos, paralisação de serviços essenciais, falhas no atendimento às áreas e desperdício de recursos por duplicidades ou aditivos emergenciais.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Centralizar o controle da gestão dos contratos e serviços de TIC.
2. Criar inventário institucional dos contratados e terceirizados.
3. Definir e divulgar o catálogo de serviços terceirizados.
4. Estabelecer indicadores de qualidade e aderência contratual.
5. Implantar sistema centralizado de gestão de contratos.

Como cada ação reduz o risco

1. Centralização → elimina perda de informações e duplicidade.
2. Inventário → reduz falhas de planejamento.

3. Catálogo → padroniza visão dos serviços.
4. Indicadores → revelam falhas rapidamente.
5. Sistema central → assegura governança contínua.

Responsável: CPROM

Situação: Planejado

KRI: % de contratos e serviços planejados conforme PTD/PDTIC por mês.

Interpretação do KRI: Mede aderência do planejamento de contratações à estratégia institucional. Percentuais baixos revelam risco direto de expiração de contratos, paralisação e retrabalho emergencial.

Fórmula: (Contratos planejados conforme PTD/PDTIC ÷ Total de contratos críticos) × 100

Meta: ≥ 95%

2.5.2 Risco: R17 – ID: CPROM-02 – Impugnações, erros e vícios em TRs por desconhecimento do objeto e demandas fora do planejamento

Tipo de Risco: Operacional

Erros, falhas e impugnações nos Termos de Referência ocorrem quando há desconhecimento técnico do objeto, ausência de padrões e demandas enviadas fora do escopo planejado, ocasionando licitações fracassadas e atrasos críticos.

Tipo de Tratamento: Aceitação e Monitoria

Plano de Tratamento

1. Criar rotina estruturada de revisão e inspeção dos TRs.
2. Verificar aderência dos TRs ao padrão institucional.

Como cada ação reduz o risco

1. Revisão → reduz erros que levam à impugnação.
2. Aderência ao padrão → padroniza qualidade e reduz inconsistências.

Responsável: CPROM

Situação: Implantado

KRI: % de TRs revisados conforme padrão por mês.

Interpretação do KRI: Mede conformidade e qualidade dos Termos de Referência. Baixa revisão aumenta risco de impugnação, licitação deserta e atraso em contratações críticas.

Fórmula: (TR revisados ÷ Total de TR emitidos) × 100

Meta: 100%

2.5.3 Risco: R18 – ID: CPROM-03 – Ilegalidades e impugnações em TRs por treinamento insuficiente nos controles legais de contratação

Tipo de Risco: Operacional

A falta de conhecimento sobre legislação, requisitos formais e padrões de contratação gera vícios, erros, ilegalidades e licitações desertas, comprometendo contratações essenciais ao TJBA.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar rotina de revisão e inspeção dos TRs.
2. Criar indicadores de aderência do TR ao padrão legal.
3. Verificar alinhamento entre demanda × planejamento de contratações.

Como cada ação reduz o risco

1. Revisão técnica → reduz erros formais.
2. Indicadores legais → aumentam segurança jurídica.
3. Alinhamento demanda × planejamento → evita retrabalho e licitações inválidas.

Responsável: CPROM

Situação: Planejado

KRI: % de TRs aderentes aos controles legais e ao planejamento por mês.

Interpretação do KRI: Indica grau de conformidade jurídica e aderência às regras de contratação. Níveis baixos refletem risco de ilegalidades, impugnações e licitações frustradas.

Fórmula: (TRs aderentes ÷ Total de TRs avaliados) × 100

Meta: ≥ 95%

2.5.4 Risco: R19 – ID: CPROM-04 – Erros ou vícios contratuais por ausência de controle das etapas formais de contratação

Tipo de Risco: Operacional

O não cumprimento integral das etapas formais de contratação (fluxos, validações, controles) gera atrasos, retrabalho, falhas contratuais e degradação da imagem da área de TIC, além de riscos legais e administrativos.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar indicadores de aderência às etapas e fluxos da contratação.
2. Realizar auditoria das etapas planejamento × execução.

Como cada ação reduz o risco

1. Indicadores → apontam falhas nas etapas.
2. Auditorias → corrigem desvios rapidamente.
3. Aderência aos fluxos → reduz riscos contratuais e operacionais.

Responsável: CPROM

Situação: Planejado

KRI: % de etapas do processo de contratação cumpridas conforme fluxo.

Interpretação do KRI: Percentual baixo indica vulnerabilidade séria ao processo, com risco de falhas, retrabalho, atrasos e inconsistências legais.

Fórmula: (Etapas cumpridas ÷ Total de etapas previstas) × 100

Meta: ≥ 98%

2.5.5 Risco: R20 – ID: CPROM-05 – Dispersão documental e inconsistências por sistemas não integrados e ausência de inventário central

Tipo de Risco: Operacional

A dispersão de documentos, ausência de inventário de serviços terceirizados e falta de integração entre sistemas geram duplicidades, falhas de fiscalização, inconsistências contratuais e perda de controle sobre serviços críticos.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Integrar sistemas de gestão de contratos e serviços terceirizados.
2. Formalizar inventário de serviços de TIC.
3. Definir política de gestão de contratos terceirizados com indicadores de aderência.

Como cada ação reduz o risco

1. Integração de sistemas → reduz falhas e inconsistências.
2. Inventário centralizado → aprimora visibilidade e priorização.
3. Política estruturada → padroniza fiscalização e qualidade.

Responsável: CPROM

Situação: Não Iniciado

KRI: % de contratos/serviços terceirizados registrados e monitorados em sistema único por mês.

Interpretação do KRI: Indica o grau de controle consolidado sobre terceirizações. Baixa cobertura revela riscos de inconsistência, descumprimento contratual e duplicidades de serviços.

Fórmula: (Contratos registrados ÷ Total de contratos ativos) × 100

Meta: 100%

3 Diretoria de Infraestrutura de TIC (DIN)

A Diretoria de Infraestrutura de TIC (DIN) é a estrutura responsável por sustentar a base tecnológica que viabiliza o funcionamento contínuo dos serviços judiciais e administrativos do TJBA. Sua atuação está diretamente relacionada à disponibilidade, segurança, capacidade, continuidade e resiliência dos ambientes críticos de tecnologia.

A DIN administra o datacenter institucional, supervisiona a rede corporativa, gerencia os ativos de infraestrutura, assegura a performance dos ambientes de produção, coordena a conectividade com todas as unidades do Tribunal, e implementa controles essenciais de segurança cibernética, identidades, replicação e contingência. Essas funções garantem que sistemas como PJe, ePROC, SEI, ERP, serviços corporativos de rede e aplicações internas permaneçam operando com estabilidade e previsibilidade.

No ciclo de análise de riscos 2026, a DIN apresentou riscos associados à capacidade do datacenter, redundância de links, continuidade tecnológica, cibersegurança avançada e controles sobre identidades e segmentação de rede, conforme matriz de riscos da planilha institucional.

Os riscos mapeados reforçam a importância estratégica da DIN no ecossistema de TIC do Tribunal, especialmente diante do crescimento acelerado das demandas digitais, da adoção de novos serviços em nuvem, da interdependência entre sistemas e da expansão do modelo de justiça digital.

3.1 Plano de Tratamento dos Riscos da Diretoria de Infraestrutura de TIC (DIN):

A DIN é responsável por garantir a infraestrutura crítica de TIC do TJBA, abrangendo datacenter, conectividade, continuidade tecnológica, segurança de rede, identidades digitais, equipamentos, e monitoramento da operação.

Trata-se de uma diretoria altamente sensível por sustentar serviços essenciais como redes corporativas, sistemas judiciais e administrativos, serviços de datacenter, ambientes de produção, links e segurança cibernética.

Principais riscos mapeados na DIN:

- Saturação ou insuficiência da capacidade do datacenter, impactando disponibilidade de serviços críticos.
- Falhas ou indisponibilidades de operadoras e links de telecom, gerando paralisação de comarcas.
- Cobertura incompleta de continuidade e replicação, expondo o TJBA a desastres físicos/lógicos.
- Ataques cibernéticos avançados por controles incompletos (rede + identidades).

3.1.1 Risco: R33 – ID: DIN-01 – Crescimento acelerado de demandas digitais excede capacidade do datacenter

Tipo de Risco: Estratégico

A capacidade limitada do datacenter, associada ao crescimento acelerado de demandas institucionais, pode causar indisponibilidade, degradação de serviços essenciais e interrupções críticas.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Instituir processo de gestão contínua de capacidade (ITIL).
2. Criar painéis de uso em tempo real (CPU, RAM, Storage, Energia).
3. Realizar testes periódicos de estresse e carga.
4. Criar política de priorização de cargas em cenários críticos.
5. Executar testes completos de DR/PCN regularmente.

Como cada ação reduz o risco

1. Monitora saturação antes de falhas.
2. Melhora previsibilidade de escassez de capacidade.
3. Testes de carga evitam interrupções reais.
4. Priorização garante continuidade de serviços essenciais.
5. DR/PCN reduz impacto de incidentes estruturais.

Responsável: DIN

Situação: Planejado

KRI: % de utilização de capacidade crítica dentro dos thresholds definidos por mês.

Interpretação do KRI: Quanto maior a violação dos thresholds, maior o risco de saturação, indisponibilidade e falhas generalizadas no datacenter.

Fórmula: (Horas dentro do threshold ÷ Horas monitoradas) × 100

Meta: ≥ 95%

3.1.2 Risco: R34 – ID: DIN-02 – Falhas de operadoras e baixa redundância de conectividade geram paralisação de comarcas

Tipo de Risco: Estratégico

Redes WAN/LAN e links de telecom apresentam pontos únicos de falha, resultando em perda de acesso a sistemas críticos e paralisação de unidades remotas.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Exigir dois links redundantes por comarca.
2. Implementar contingência móvel (4G/5G).
3. Criar NOC unificado com dashboards de disponibilidade.
4. Implementar SLAs e penalidades robustas.
5. Integrar procedimentos de resposta a incidentes ao ITSM.

Como cada ação reduz o risco

1. Redundância → elimina pontos únicos de falha.
2. Contingência → mantém serviços mínimos em incidentes.
3. NOC → reduz tempo de detecção e resposta.
4. SLAs → incentivam operadoras a manter qualidade.

Responsável: DIN

Situação: Em Implantação

KRI: % de comarcas com conectividade redundante ativa por mês.

Interpretação do KRI: Percentual baixo indica exposição crítica: basta um incidente para paralisar unidades inteiras.

Fórmula: (Comarcas com redundância ÷ Total de comarcas) × 100

Meta: 100%

3.1.3 Risco: R35 – ID: DIN-03 – Cobertura incompleta de continuidade e replicação para serviços essenciais

Tipo de Risco: Estratégico

A continuidade de TIC é limitada devido à ausência de replicação completa e matriz RTO/RPO definida, expondo o TJBA a interrupções prolongadas em caso de desastres físicos ou lógicos.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Finalizar matriz RTO/RPO de sistemas críticos.
2. Implantar replicação automática e contínua.
3. Realizar testes completos de DR com restauração real.
4. Criar runbooks de recuperação.
5. Implantar indicador estratégico de cobertura de DR.

Como cada ação reduz o risco

1. RTO/RPO → define capacidade de recuperação.
2. Replicação → previne perda de dados.
3. Testes → validam eficácia real do plano.
4. Runbooks → garantem resposta organizada.

Responsável: DIN

Situação: Em implantação

KRI: % de sistemas críticos cobertos por DR testado por mês.

Interpretação do KRI: Mostra real nível de resiliência. Percentual baixo indica risco extremo de paralisação institucional.

Fórmula: (Sistemas com DR testado ÷ Total de sistemas críticos) × 100

Meta: ≥ 90%

3.1.4 Risco: R36 – ID: DIN-04 – Ataques cibernéticos avançados por controles incompletos de identidade e rede

Tipo de Risco: Estratégico

Os controles de identidade (IGA, MFA) e segmentação de rede estão parcialmente implementados, possibilitando ataques cibernéticos sofisticados, vazamento de dados e indisponibilidade de serviços essenciais.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Tornar MFA obrigatório para sistemas críticos.
2. Concluir a implantação de IGA com SoD.
3. Implementar SOC/SIEM com resposta rápida.
4. Implantar gestão contínua de vulnerabilidades.
5. Reforçar campanhas permanentes de sensibilização.

Como cada ação reduz o risco

1. MFA → bloqueia acessos indevidos.
2. IGA → reduz privilégios excessivos.
3. SOC → detecta invasões.
4. Vulnerability Management → reduz superfície de ataque.

Responsável: DIN

Situação: Planejado

KRI: % de identidades críticas com MFA + IGA completos por mês.

Interpretação do KRI: Indicador crítico da postura de segurança. Baixa aderência aumenta risco de ataques avançados, sequestro de contas e interrupção de serviços essenciais.

Fórmula: (Identidades com MFA+IGA completas ÷ Total de identidades críticas) × 100

Meta: 100%

3.2 Plano de Tratamento dos Riscos da Coordenação de Tecnologia e Infraestrutura de TIC (COTEC):

A COTEC gerencia a infraestrutura física e lógica de TIC, incluindo servidores, clusters, sistemas operacionais, patching, legados, automação de correções, governança de nuvem e continuidade técnica.

Principais riscos mapeados:

- Falhas físicas em cluster por ausência de garantia e peças.
- Sistema operacional do cluster desatualizado (risco de bug crítico).
- Vulnerabilidades em sistemas legados por falha de correção.
- Ausência de patch management automatizado

3.2.1 Risco: R56 – ID: COTEC-01 – Falha física do cluster por ausência de garantia e peças

Tipo de Risco: Tático

Sem garantia vigente e estoque suficiente, falhas físicas de cluster podem causar indisponibilidade de serviços essenciais.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Renovar o parque tecnológico com novos equipamentos com garantia vigente;
2. E/ou prorrogar contratos de suporte e manutenção antes do vencimento;
3. Garantir estoque de peças sobressalentes e cobertura com fornecedores;
4. Realizar verificações periódicas de validade dos contratos;
5. Integrar indicadores de garantia na governança da infraestrutura.

Como cada ação reduz o risco

1. Renovação de contrato/garantia: reduz risco de paralisação em caso de falha física.
2. Estoque de peças: possibilita substituição imediata e reduz tempo de indisponibilidade.
3. Verificação periódica: evita janelas de exposição entre vencimento e renovação contratual.
4. Indicadores de garantia: aumentam visibilidade executiva sobre riscos estruturais.

Responsável: COTEC

Situação: Em Execução

KRI: % de equipamentos do cluster com garantia vigente por mês.

Interpretação do KRI: Mostra o grau de exposição do cluster. Baixa cobertura indica risco elevado de falha física sem suporte, podendo causar interrupção generalizada de serviços.

Fórmula:(Quantidade de equipamentos do cluster com garantia vigente ÷ Total de equipamentos do cluster) × 100

Meta: ≥ 95%

3.2.2 Risco: R57 – ID: COTEC-02 – Erro crítico de SO do cluster por sistema operacional desatualizado

Tipo de Risco: Tático

O sistema operacional do cluster encontra-se desatualizado, aumentando a probabilidade de falhas, bugs, vulnerabilidades críticas e indisponibilidade de serviços essenciais.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Atualizar periodicamente o SO do hypervisor do cluster utilizando o contrato de garantia de software;
2. Estabelecer rotina de atualização periódica e obrigatória;
3. Criar janelas de atualização alinhadas ao calendário de manutenção;
4. Integrar controle de atualização ao painel de gestão de infraestrutura.

Como cada ação reduz o risco

1. Atualizações frequentes: eliminam bugs conhecidos e falhas de segurança;
2. Janelas planejadas: evitam indisponibilidades inesperadas;
3. Painel de governança: permite acompanhar e corrigir atrasos;
4. Uso do contrato de software: reduz risco financeiro e operacional.

Responsável: COTEC

Situação: Em Execução

KRI: Idade média da última atualização do SO no semestre.

Interpretação do KRI: Quanto maior a idade desde a última atualização, maior o risco de falhas críticas e vulnerabilidades não corrigidas.

Fórmula: Soma dos meses desde última atualização ÷ nº de nós

Meta: ≤ 3 meses

3.2.3 Risco: R58 – ID: COTEC-03 – Vulnerabilidades em sistemas legados não corrigidas

Tipo de Risco: Tático

Sistemas legados com falhas conhecidas e sem correção tornam-se alvos fáceis para exploração, podendo causar incidentes de segurança, indisponibilidade e degradação do ambiente de produção.

Tipo de Tratamento: Controles Detectivos e Corretivo

Plano de Tratamento

1. Criar plano conjunto COTEC + Desenvolvimento para correção dos sistemas legados;
2. Priorizar sistemas críticos e organizar cronograma de correção;
3. Implementar verificações periódicas de vulnerabilidades;
4. Integrar resultados no ciclo de gestão de riscos de TIC.

Como cada ação reduz o risco

1. Correção coordenada: reduz lacunas entre infraestrutura e desenvolvimento;
2. Priorização de sistemas críticos: minimiza impactos dos maiores riscos;
3. Verificações contínuas: previnem reincidência de falhas;
4. Integração ao ciclo de riscos: fortalece governança.

Responsável: COTEC

Situação: Planejado

KRI: % de servidores com patches críticos aplicados dentro do SLA no mês.

Interpretação do KRI: Quanto menor a taxa de correção, maior o risco de exploração e incidentes de segurança.

Fórmula:(N° de servidores com patches críticos aplicados dentro do prazo ÷ N° total de servidores com patches críticos identificados) × 100

Meta: ≥ 95%

3.2.4 Risco: R59 – ID: COTEC-04 – Exploração de vulnerabilidades por falta de solução automatizada de correção (patch management)

Tipo de Risco: Operacional

A ausência de ferramenta de patch management impede correção rápida de vulnerabilidades críticas, gerando risco de exploração, falhas e indisponibilidade dos serviços.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Adquirir e implantar ferramenta de patch management;
2. Estabelecer SLAs de correção por criticidade;
3. Integrar o patch management ao SOC/SIEM;
4. Produzir relatórios periódicos de vulnerabilidades corrigidas.

Como cada ação reduz o risco

1. Automação: acelera correções críticas;
2. SLAs: garantem prazos curtos de mitigação;
3. Integração ao SOC: aumenta visibilidade;
4. Relatórios: fortalecem governança.

Responsável: COTEC

Situação: Não Iniciado

KRI: % de vulnerabilidades críticas corrigidas no período por mês.

Interpretação do KRI: Mostra a velocidade de reação a vulnerabilidades graves. Baixos índices indicam risco real de ataque.

Fórmula:(Vulnerabilidades críticas corrigidas ÷ Total de vulnerabilidades críticas identificadas) × 100

Meta: ≥ 95%

3.2.5 Risco: R60 – ID: COTEC-05 – Descontrole de consumo e aumento súbito de uso de serviços em nuvem por falta de governança FinOps

Tipo de Risco: Operacional

A ausência de limitação efetiva e governança formal do consumo de serviços em nuvem pode causar exaustão financeira do contrato, resultando em paralisação de serviços e impacto crítico às operações.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Fortalecer governança de adoção de serviços em nuvem;
2. Ampliar thresholds com políticas de bloqueio;
3. Adotar práticas formais de FinOps;
4. Implementar dashboards de uso e projeção de custos;
5. Criar alertas automáticos por faixa de consumo.

Como cada ação reduz o risco

1. FinOps: dá previsibilidade e controle financeiro;
2. Thresholds com bloqueio: evitam estouros inesperados;
3. Dashboards: aumentam visibilidade do consumo;
4. Alertas: evitam riscos por aumento súbito.

Responsável: COTEC

Situação: Planejado

KRI: % de consumo do orçamento anual de serviços em nuvem por mês.

Interpretação do KRI: Indica exposição ao esgotamento contratual. Percentuais muito altos rapidamente sugerem risco de interrupção dos serviços.

Fórmula:(Valor consumido ÷ Orçamento anual de nuvem) × 100

Meta: ≤ 50% até metade do exercício e ≤ 90% até o final do ano

3.3 Plano de Tratamento dos Riscos da Coordenação de Atendimento, Soluções de Usuário e Equipamentos de TIC (COATE):

A Coordenação de Atendimento e Equipamentos, COATE, também atua como núcleo de governança operacional de suporte, incidentes, catálogo, ativos e patrimônio de TI e é responsável pela operação diária dos serviços de suporte técnico aos usuários, gestão de incidentes, manutenção e distribuição de equipamentos, governança de ativos, catálogo de serviços, atendimento a entidades externas, gestão de demandas e conformidade operacional dos serviços de TI prestados pela SETIM.

Os riscos mapeados nesta coordenação refletem diretamente a qualidade do atendimento, a padronização das práticas operacionais, a confiabilidade dos ativos de TI, a privacidade dos dados manipulados no suporte, e a adequação dos processos à carga de trabalho crescente.

Principais riscos mapeados da COATE:

- Atrasos e paralisações por falta de planejamento ou estoque insuficiente de equipamentos.
- Perda de conhecimento técnico por dependência de terceiros e falta de documentação.

- Sobrecarga da equipe causando backlog, estouro de SLA e baixa qualidade.
- Base de conhecimento incompleta, gerando erros repetidos e retrabalho.
- Falhas no atendimento a entidades externas, com impacto institucional e reputacional.
- Catálogo de serviços desatualizado, dificultando classificação e resolução de chamados.
- Fragmentação e conflito no uso da ferramenta ITSM, comprometendo a governança ITIL.
- Riscos de privacidade e vazamentos de dados no suporte remoto.
- Falhas em fiscalização de contratos, gestão patrimonial e controle de acessos.

3.3.1 Risco: R37 – ID: COATE-01 – Atrasos de fornecedores de equipamentos por falta de planejamento de aquisição

Tipo de Risco: Tático

A ausência de planejamento plurianual adequado para aquisição de equipamentos de TIC gera atraso nas entregas, causando paralisação de serviços, indisponibilidade de estações de trabalho e impacto direto na produtividade dos usuários e das áreas técnicas.

Tipo de Tratamento: Controles Aceitação e Monitoria

Plano de Tratamento

1. Formalizar política/procedimento de planejamento plurianual de aquisições, definindo níveis mínimos de estoque;
2. Integrar planejamento de compras à gestão de patrimônio;
3. Criar relatórios periódicos de status de pedidos;
4. Definir controles de acompanhamento de fornecedores.

Como cada ação reduz o risco

1. Política formal → reduz improviso e atrasos recorrentes.
2. Integração com patrimônio → melhora previsão de demanda real.
3. Relatórios periódicos → permitem intervenção antes de impactos críticos.
4. Controles de fornecedores → aumentam previsibilidade nas entregas.

Responsável: COATE

Situação: Planejado

KRI: % de pedidos de equipamentos entregues fora do prazo contratual trimestralmente.

Interpretação do KRI: Indica a confiabilidade do processo de aquisição. Quanto maior o percentual de atrasos, maior o risco de paralisação operacional.

Fórmula:(N° de pedidos entregues com atraso ÷ N° total de pedidos entregues) × 100

Meta: ≤ 5%

3.3.2 Risco: R38 – ID: COATE-02 – Falta de recursos de equipamentos por reserva técnica insuficiente

Tipo de Risco: Tático

A reserva técnica de equipamentos é insuficiente, causando atrasos no atendimento, paralisação de usuários e imposição de soluções improvisadas.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Definir política formal de reserva técnica, com parâmetros de estoque mínimo;
2. Registrar e controlar estoques em sistema;
3. Criar alertas automáticos de baixa de estoque.

Como cada ação reduz o risco

1. Estoque mínimo → reduz paralisações;
2. Registro em sistema → impede falhas de inventário;
3. Alertas → evitam rupturas de estoque.

Responsável: COATE

Situação: Planejado

KRI: % de cobertura de reserva técnica por mês.

Interpretação do KRI: Mostra a capacidade da COATE de repor equipamentos rapidamente. Baixa cobertura indica risco de interrupção dos serviços.

Fórmula:(Equipamentos em reserva ÷ Equipamentos em produção) × 100

Meta: 10–15% nas categorias críticas

3.3.3 Risco: R39 – ID: COATE-03 – Perda de conhecimento técnico por dependência de terceiros

Tipo de Risco: Tático

A dependência do conhecimento não documentado de terceiros gera riscos de retrabalho, erros, atrasos e baixa qualidade, especialmente quando equipes de fornecedores mudam.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implantar processo formal de Gestão do Conhecimento de Terceiros;
2. Criar requisitos contratuais de entrega de documentação técnica;
3. Criar repositório corporativo (wiki/GC);
4. Implantar checklists de transição e auditorias de cobertura.

Como cada ação reduz o risco

1. Documentação técnica → reduz dependência de pessoas;
2. Checklists → eliminam lacunas de transição;
3. Auditorias → asseguram que conhecimento está completo;
4. Repositório único → evita perda de informação.

Responsável: COATE

Situação: Planejado

KRI: % de serviços/processos críticos com documentação completa por mês.

Interpretação do KRI: Indica maturidade da gestão de conhecimento. Baixo percentual significa risco de falhas após turnover.

Fórmula: (N° de serviços/processos críticos documentados ÷ Total de processos críticos) × 100

Meta: ≥ 90%

3.3.4 Risco: R40 – ID: COATE-04 – Sobrecarga e excesso de demandas por ausência de gestão de capacidade produtiva

Tipo de Risco: Tático

A falta de mecanismos estruturados de gestão da capacidade cria filas, estouro de SLA, perda de qualidade, insatisfação do usuário e sobrecarga da equipe.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Implementar gestão da capacidade produtiva;
2. Definir indicadores de carga por equipe;
3. Estabelecer limites de backlog;
4. Criar relatórios mensais para diretoria.

Como cada ação reduz o risco

1. Indicadores → mostram saturação;
2. Limites → evitam colapso operacional;
3. Relatórios → promovem decisões corretivas tempestivas.

Responsável: COATE

Situação: Não Iniciado

KRI: Backlog relativo mensal (Fórmula: chamados pendentes no mês ÷ capacidade mensal).

Interpretação do KRI: Mostra desbalanceamento entre demanda e capacidade. Valores altos indicam risco direto de rupturas de SLA.

Meta: ≤ 1,0 (ideal ≤ 0,5)

3.3.5 Risco: R41 – ID: COATE-05 – Base de conhecimento incompleta causa retrabalho e falhas

Tipo de Risco: Tático

A falta de governança sobre a Base de Conhecimento resulta em soluções inadequadas, erros recorrentes, retrabalho e insatisfação do usuário.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar governança da base de conhecimento;
2. Definir donos por área;
3. Criar workflow de publicação;
4. Revisar periodicamente artigos críticos;
5. Implantar indicadores de uso.

Como cada ação reduz o risco

1. Donos de processo → garantem qualidade;
2. Revisões → evitam artigos desatualizados;
3. Indicadores → mostram efetividade da base.

Responsável: COATE

Situação: Planejado

KRI: % de incidentes resolvidos com uso da base de conhecimento a cada trimestre.

Interpretação do KRI: Quanto maior o uso da base, menor a recorrência de falhas e menores os tempos de solução.

Meta: ≥ 60–70%

3.3.6 Risco: R42 – ID: COATE-06 – Falhas e atrasos no atendimento a entidades externas por procedimentos insuficientes

Tipo de Risco: Tático

Fluxos insuficientes para atendimento às entidades externas geram falhas, atrasos, insatisfação institucional e riscos reputacionais.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Desenhar fluxos específicos de atendimento;
2. Criar SLAs claros;
3. Definir scripts padronizados;
4. Integrar com CGTIC quando necessário;
5. Monitoramento diferenciado.

Como cada ação reduz o risco

1. Fluxos definidos → reduzem falhas;

2. SLAs → disciplinam o tempo de resposta;
3. Integração → reduz ruídos operacionais.

Responsável: COATE

Situação: Em execução

KRI: % de demandas externas atendidas dentro do prazo por mês.

Interpretação do KRI: Mede aderência ao serviço prestado às entidades externas. Baixo percentual compromete a imagem institucional.

Fórmula:(Demandas atendidas dentro do prazo ÷ Total de demandas externas) × 100

Meta: ≥ 95%

3.3.7 Risco: R43 – ID: COATE-07 – Erros, desatualização e conflitos no Catálogo de Serviços TIC por desalinhamento e não atualização

Tipo de Risco: Tático

O catálogo de serviços TIC, utilizado pelos usuários e pela própria operação, encontra-se sujeito a erros, desatualização, inconsistências e divergências entre o catálogo técnico (mantido pela CGTIC) e o catálogo orientado ao usuário (COATE).

Esse desalinhamento prejudica:

- A correta classificação de chamados,
- A identificação de responsáveis,
- A priorização adequada,
- A experiência dos usuários, e
- A eficiência do atendimento, resultando em prazos maiores, retrabalho e aumento de insatisfação.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar um processo formal de gestão do catálogo, prevendo gatilho obrigatório de atualização sempre que um novo serviço técnico for implantado pela CGTIC.
2. Criar um checklist de alinhamento entre catálogo técnico e catálogo para o usuário.
3. Implantar revisões trimestrais obrigatórias para manutenção do catálogo.
4. Instituir comitê conjunto CGTIC + COATE para homologação de atualizações.
5. Documentar responsáveis pela atualização de cada entrada de serviço.

Como cada ação reduz o risco

1. Processo formal → elimina lacunas e atualizações ad hoc.
2. Checklists de alinhamento → evitam divergências entre catálogos.
3. Revisões trimestrais → garantem atualização contínua.
4. Comitê conjunto → garante coerência entre visão técnica e visão de atendimento.

5. Responsáveis definidos → evita que serviços "entrem em operação" sem serem catalogados.

Responsável: COATE

Situação: Em Execução

KRI: % de chamados abertos em categorias "outros" ou "não identificado" no mês.

Interpretação do KRI: Um número elevado de chamados classificados em categorias genéricas indica falha no catálogo, pois o usuário (ou o atendente) não encontra o serviço correto. Isso impacta:

- Qualidade do atendimento,
- Roteamento adequado,
- Aderência do catálogo às operações reais,
- Maturidade do processo ITSM.

Valores altos do KRI são evidência clara de catálogo desatualizado ou inconsistente.

Fórmula: (N° de chamados em categorias genéricas ÷ N° total de chamados abertos no mês) × 100

Meta: ≤ 5%

3.3.8 Risco: R44 – ID: COATE-08 – Fragmentação, retrabalho e conflitos no uso da ferramenta ITSM por falta de governança integrada

Tipo de Risco: Tático

A falta de alinhamento entre COATE e CGTIC sobre processos ITSM gera fragmentação da operação, rotas de atendimento divergentes, categorização incorreta, retrabalho, perda de dados de atendimento e redução da maturidade ITIL.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar comitê permanente COATE × CGTIC para governança ITSM;
2. Definir papéis e responsabilidades entre equipes (RACI ITSM);
3. Alinhar processos da ferramenta ao processo mapeado na CGTIC;
4. Publicar fluxos e instruções operacionais;
5. Realizar alinhamentos mensais de operação.

Como cada ação reduz o risco

1. Comitê → reduz conflitos e ruídos operacionais;
2. RACI → esclarece responsabilidades;
3. Aderência ao processo mapeado → aumenta maturidade ITIL;
4. Instruções → reduzem inconsistências no uso da ferramenta.

Responsável: COATE

Situação: Não Iniciado

KRI: % de processos ITIL implementados no ITSM trimestralmente.

Interpretação do KRI: Quanto menor a implementação, maior a fragmentação, inconsistência e retrabalho.

Fórmula: (Processos ITIL implementados ÷ Total de processos ITIL aplicáveis) × 100

Meta: ≥ 80%

3.3.9 Risco: R45 – ID: COATE-09 – Falhas de telefonia e paralisação de atendimento por dependência de terceiros e ausência de monitoramento

Tipo de Risco: Operacional

Telefonia institucional depende de fornecedores externos, sem mecanismos completos de redundância ou monitoramento, causando indisponibilidade de atendimento, inclusive para comarcas.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Estabelecer plano de contingência da telefonia;
2. Criar relatórios de disponibilidade;
3. Implementar monitoramento ativo (NOC);
4. Exigir SLAs e penalidades.

Como cada ação reduz o risco

1. Contingência → minimiza impacto de falhas;
2. Monitoramento → acelera diagnóstico;
3. SLAs → aumentam confiabilidade do fornecedor.

Responsável: COATE

Situação: Não Iniciado

KRI: Tempo de indisponibilidade mensal de telefonia.

Interpretação do KRI: Quanto maior, maior impacto direto no atendimento institucional.

Meta: ≤ 30 minutos/mês

3.3.10 Risco: R46 – ID: COATE-10 – Falhas no Catálogo Técnico × Catálogo do Usuário por falta de integração

Tipo de Risco: Operacional

Divergências entre catálogo técnico e catálogo do usuário prejudicam classificação, SLA, encaminhamento e tempo de resolução dos chamados.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar workflow integrado para atualizações;
2. Verificar aderência mensal entre ambos os catálogos;
3. Definir responsáveis pela atualização cruzada;
4. Criar alertas quando serviços forem alterados.

Como cada ação reduz o risco

1. Workflow → evita divergências;
2. Aderência mensal → reduz falhas operacionais;
3. Responsáveis → eliminam lacunas.

Responsável: COATE

Situação: Em Execução

KRI: % de serviços do catálogo técnico alinhados ao catálogo do usuário por mês.

Interpretação do KRI: Baixa aderência indica riscos de erro e retrabalho.

Meta: ≥ 90%

3.3.11 Risco: R47 – ID: COATE-11 – Vulnerabilidades de privacidade no suporte remoto por ausência de consentimento formal

Tipo de Risco: Operacional

O suporte remoto realizado sem consentimento formal do usuário gera risco de violação de privacidade, exposição indevida de dados e não conformidade com LGPD.

Tipo de Tratamento: Controles Preventivo e Detectivo

Plano de Tratamento

1. Exigir consentimento explícito no início da sessão;
2. Criar registro automático do consentimento;
3. Treinar a equipe em privacidade;
4. Integrar o consentimento ao ITSM.

Como cada ação reduz o risco

1. Consentimento → elimina violações legais;
2. Registro automático → cria trilha de auditoria;
3. Treinamento → reduz erros humanos.

Responsável: COATE

Situação: Em Execução

KRI: % de sessões de suporte remoto com consentimento registrado no mês.

Interpretação do KRI: Baixa conformidade indica risco direto de violação LGPD.

Meta: 100%

3.3.12 Risco: R48 – ID: COATE-12 – Desvios, inconsistências e retrabalho por requisições fora do padrão

Tipo de Risco: Operacional

Requisições feitas fora do padrão causam retrabalho, erros, perda de rastreabilidade e aumento do tempo de atendimento.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar padrões de requisições;
2. Integrar padrões ao catálogo do usuário;
3. Definir regras de rejeição automática;
4. Treinar usuários.

Como cada ação reduz o risco

1. Padrões → evitam retrabalho;
2. Rejeição automática → reduz inconsistências;
3. Treinamento → aumenta aderência.

Responsável: COATE

Situação: Planejado

KRI: % de requisições aderentes ao padrão por mês.

Interpretação do KRI: Quanto menor o percentual, maior o retrabalho operacional.

Meta: ≥ 90%

3.3.13 Risco: R49 – ID: COATE-13 – Falhas na fiscalização e não conformidade de contratos por insuficiência de governança

Tipo de Risco: Operacional

A falta de mecanismos de governança e acompanhamento de fiscais de contratos gera riscos de inadimplência, perda de qualidade, pagamentos indevidos e penalidades.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar matriz de fiscalização obrigatória;
2. Exigir plano mensal de fiscalização dos fiscais;
3. Registrar fiscalizações em sistema;
4. Criar trilha de capacitação.

Como cada ação reduz o risco

1. Matriz → garante cobertura completa;
2. Registro → aumenta rastreabilidade;

3. Capacitação → reduz falhas de fiscalização.

Responsável: COATE

Situação: Planejado

KRI: % de contratos com fiscalização em dia por mês.

Interpretação do KRI: Indica o grau de governança contratual. Baixa aderência aumenta risco de falhas e penalidades.

Meta: ≥ 95%

3.3.14 Risco: R50 – ID: COATE-14 – Ilegalidades em contratos por falta de capacitação dos fiscais

Tipo de Risco: Operacional

Fiscais sem treinamento adequado geram risco de falhas de fiscalização, descumprimento contratual, apontamentos e responsabilizações.

Tipo de Tratamento: Controles Preventivo e Detectivo

Plano de Tratamento

1. Criar trilha de capacitação para fiscais;
2. Implantar certificação anual;
3. Criar painel de fiscais capacitados.

Como cada ação reduz o risco

1. Capacitação → reduz erros;
2. Certificação → garante atualização contínua.

Responsável: COATE

Situação: Não Iniciado

KRI: % de fiscais treinados e certificados no ano.

Interpretação do KRI: Indica aderência ao processo e segurança jurídica.

Meta: 100%

3.3.15 Risco: R51 – ID: COATE-15 – Indisponibilidade e degradação de canais de atendimento

Tipo de Risco: Operacional

Canais de atendimento (chat, telefone, portal, e-mail) podem operar de forma instável ou lenta, degradando a experiência do usuário e gerando atraso no atendimento.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar Painel de observabilidade dos canais;
2. Monitorar disponibilidade;
3. Registrar incidentes e tratativas.

Como cada ação reduz o risco

1. Observabilidade → permite atuação proativa;
2. Registro → identifica padrões de falhas.

Responsável: COATE

Situação: Planejado

KRI: Disponibilidade mensal dos canais.

Interpretação do KRI: Baixa disponibilidade indica risco direto à prestação de serviços.

Meta: ≥ 99%

3.3.16 Risco: R52 – ID: COATE-16 – Incidentes de privacidade em equipamentos de usuários

Tipo de Risco: Operacional

Equipamentos manuseados pelo suporte podem conter dados sensíveis, criando risco de incidentes de privacidade.

Tipo de Tratamento: Controles Preventivos

Plano de Tratamento

1. Criar procedimento formal de atendimento com dados sensíveis;
2. Treinar equipe;
3. Criar evidências de limpeza/segurança.

Como cada ação reduz o risco

1. Procedimentos → padronizam segurança;
2. Treinamento → reduz erros;
3. Evidências → fortalecem auditoria.

Responsável: COATE

Situação: Planejado

KRI: N° de incidentes de privacidade relacionados ao atendimento no mês.

Interpretação do KRI: Qualquer valor > 0 é crítico.

Meta: 0 incidentes

3.3.17 Risco: R53 – ID: COATE-17 – Perda, mau uso e inconsistências patrimoniais em equipamentos de informática

Tipo de Risco: Operacional

A gestão patrimonial de equipamentos de TIC apresenta falhas como registros desatualizados, movimentações sem formalização e ausência de conciliações periódicas.

Isso gera riscos de perda de equipamentos, uso indevido, divergências patrimoniais, sanções administrativas, e falhas no atendimento quando o patrimônio não corresponde ao real inventário.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implementar fluxo integrado COATE × Patrimônio institucional, com registro obrigatório de entrada, saída, troca e recolhimento de equipamentos.
2. Implantar inventário eletrônico centralizado com dados de número de série, etiqueta, unidade, responsáveis e histórico.
3. Realizar conferência anual completa e conferências trimestrais por amostragem.
4. Criar responsáveis patrimoniais por unidade/setor ("focais patrimoniais").
5. Integrar a movimentação de patrimônio com os processos de suporte técnico (ITSM), evitando informalidades.
6. Registrar movimentações através de ordens de serviço formalmente encerradas, impedindo repasses manuais.

Como cada ação reduz o risco

1. Fluxo integrado: elimina brechas de movimentações informais.
2. Inventário eletrônico: garante rastreabilidade completa e audível.
3. Conferências periódicas: identificam inconsistências precocemente.
4. Responsáveis locais: aumentam governança e responsabilidade descentralizada.
5. Integração com ITSM: impede que trocas ocorram sem registro formal.
6. Ordens de serviço: criam trilha de auditoria para cada movimentação de equipamento.

Responsável: COATE

Situação: Planejado

KRI: % de registros patrimoniais formalizados no sistema no mês.

Interpretação do KRI: Indica a precisão do controle patrimonial. Percentuais baixos representam alto risco de perda de bens, equipamentos desaparecidos, uso indevido e inconsistências administrativas.

Fórmula: KRI= (N° de equipamentos com registro patrimonial formalizado / Total de equipamentos em uso) × 100

Meta: ≥ 95%

3.3.18 Risco: R54 – ID: COATE-18 – Falhas e riscos de segurança por controle insuficiente de contas e acessos administrativos

Tipo de Risco: Operacional

A ausência de governança formal sobre acessos administrativos, contas privilegiadas, concessões provisórias e contas inativas expõe o TJBA a riscos de:

- Uso indevido de contas administrativas;
- Acessos acima da necessidade (privilégios excessivos);
- Falhas de rastreabilidade e ausência de trilha de auditoria;
- Não conformidade com exigências de segurança.

Tipo de Tratamento: Controles Detectivos e Preventivos

Plano de Tratamento

1. Criar Política de Governança de Acessos Administrativos, definindo níveis, critérios e responsabilidades.
2. Criar e manter matriz SoD (Segregation of Duties) revisada trimestralmente.
3. Implementar processo de recertificação periódica de acessos (trimestral para críticos).
4. Integrar acessos ao fluxo ITSM para aprovação formal e trilha de auditoria.
5. Criar rotina de cancelamento de acessos após mudança de função/lotação.
6. Criar relatórios de contas privilegiadas ativas × necessárias.

Como cada ação reduz o risco

1. Política formal: elimina concessões ad hoc.
2. SoD: reduz riscos de abuso de função e conflitos de interesse.
3. Recertificação: garante que apenas acessos necessários permaneçam ativos.
4. Trilha de auditoria: aumenta transparência e responsabilização.
5. Relatórios periódicos: identificam rapidamente acessos excessivos.

Responsável: COATE

Situação: Planejado

KRI: % de contas privilegiadas recertificadas dentro do prazo no trimestre.

Interpretação do KRI: Indica a maturidade da governança de acessos. Números baixos representam risco real de violação de segurança e uso indevido.

Fórmula: KRI = (Contas privilegiadas recertificadas no prazo / Total de contas privilegiadas ativas) × 100

Meta: ≥ 95%

3.3.19 Risco: R55 – ID: COATE-19 – Fragmentação operacional por ausência de documentação e falta de governança nos processos de suporte

Tipo de Risco: Operacional

A falta de documentação formal dos processos de suporte e a inexistência de governança de atualização geram perda de conhecimento, retrabalho, inconsistências no atendimento, variação de procedimentos entre técnicos e risco de falhas recorrentes.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar diretório único corporativo (wiki/Confluence) com versionamento.
2. Documentar todos os processos de suporte (nível 1, 2 e 3).
3. Definir donos de processo (Donos de Processo) e periodicidade de revisão.
4. Criar checklists operacionais vinculados às etapas do ITSM.
5. Implantar auditorias semestrais de conformidade processual.
6. Integrar novos artigos com a base de conhecimento.

Como cada ação reduz o risco

1. Diretório único: elimina dispersão documental.
2. Documentação padronizada: reduz divergência operacional.
3. Donos de processo: garantem gestão contínua.
4. Auditorias: asseguram atualização permanente.
5. Integração com BK: melhora tempo de resolução e reduz falhas repetida.

Responsável: COATE

Situação: Não Iniciado

KRI: % de processos documentados e revisados dentro da periodicidade no semestre.

Interpretação do KRI: Mede a maturidade operacional da COATE. Percentuais baixos indicam risco de retrabalho, perda de conhecimento e execução divergente das rotinas.

Fórmula: KRI = (Processos documentados e revisados no período / Total de processos mapeados) × 100

Meta: ≥ 95%

3.4 Plano de Tratamento dos Riscos da Coordenação Datacenter, Infraestrutura de Rede e Produção de TIC (CODAT/CPROD):

A CODAT/CPROD é responsável pela sustentação dos ambientes críticos que suportam todos os serviços de TIC do TJBA, incluindo datacenter principal, operação de produção, continuidade tecnológica, infraestrutura de rede, contratos críticos, estoque de equipamentos de infraestrutura, fitas e backups, além da gestão da capacidade técnica dos servidores de infraestrutura.

Os riscos mapeados para a CODAT/CPROD evidenciam pontos de vulnerabilidade estrutural, tais como:

- Dependência de um único datacenter, sem contingência completa;
- Riscos contratuais críticos (falência de fornecedor, deserto de licitações);
- Falta de redundância de rede em unidades;
- Estoque mínimo incapaz de absorver variações de demanda;
- Dispersão de documentos contratuais e ausência de um sistema único;
- Riscos físicos a fitas e backup legados;
- Switches críticos sem garantia;
- Sobrecarga da capacidade da equipe técnica;

3.4.1 R61 – ID: CPROD-01 – Falha grave ou desastre no Datacenter Principal por ausência de solução de continuidade (site backup ou nuvem)

Tipo de Risco: Estratégico

O TJBA opera majoritariamente em um único datacenter, o que representa risco extremo de indisponibilidade total de sistemas, paralisação de atividades judiciais/administrativas, perda de dados e degradação severa dos serviços, caso ocorra um desastre físico ou lógico.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Concluir projetos já planejados de continuidade tecnológica (migração parcial à nuvem e/ou implantação de site backup).
2. Formalizar o Plano de Continuidade de TIC (PCTIC) incluindo definição de RTO/RPO por sistema.
3. Integrar o risco ao mapa estratégico de riscos da SETIM.
4. Criar procedimentos de teste periódico de recuperação.
5. Criar inventário de sistemas críticos e classificá-los por prioridade de recuperação.

Como cada ação reduz o risco

1. Continuidade (DR/nuvem): reduz impacto de desastres e garante restauração.
2. RTO/RPO: define tempos máximos aceitáveis de parada.
3. Testes: asseguram eficácia real do plano.
4. Inventário de criticidade: permite recuperar primeiro os sistemas essenciais.

Responsável: CODAT

Situação: Planejado

KRI: % de sistemas críticos cobertos por solução de continuidade testada no trimestre.

Interpretação do KRI: Percentual baixo indica risco extremo de paralisação institucional em eventos de falha.

Fórmula:KRI=(Sistemas críticos com DR testado/ Total de sistemas críticos) ×100

Meta: ≥ 80%

3.4.2 Risco: R62 – ID: CPROD-02 – Falência ou incapacidade financeira de fornecedor crítico / Deserto de licitações por exigências excessivas

Tipo de Risco: Estratégico

Contratos críticos da infraestrutura dependem de poucos fornecedores especializados. A falência de um deles ou um certame deserto pode causar interrupção de serviços essenciais, paralisação de manutenção, impossibilidade de substituição de peças, e riscos legais para o Tribunal.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Diversificar fornecedores e criar matriz de risco contratual.
2. Revisar editais e reduzir exigências restritivas.
3. Criar plano de contingência por fornecedor crítico.
4. Monitorar periodicamente a "saúde financeira" dos fornecedores.

Como cada ação reduz o risco

1. Diversificação: reduz dependência.
2. Editais mais inclusivos: reduzem risco de licitação deserta.
3. Contingência: permite continuidade temporária.
4. Monitoramento econômico: antecipa riscos contratuais.

Responsável: CODAT

Situação: Planejado

KRI: % de contratos críticos com fornecedor em risco (financeiro ou operacional) no mês.

Interpretação do KRI: Percentual > 0 indica risco real e iminente de descontinuidade.

Fórmula: KRI= (Contratos identificados com fornecedor em risco / Total de contratos críticos) ×100

Meta: 0%

3.4.3 Risco: R63 – ID: CPROD-03 – Falha geral de infraestrutura de rede por falta de redundância mínima em unidades do TJBA

Tipo de Risco: Tático

Unidades judiciais e administrativas não possuem redundância mínima de rede, deixando-as vulneráveis a paralisação completa, perdas de comunicação e suspensão de serviços.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Completar inventário da infraestrutura de rede por unidade.
2. Definir critérios objetivos de investimento e priorização.
3. Criar plano de adequação para unidades críticas.
4. Reportar à governança o risco de continuidade.

Como cada ação reduz o risco

1. Inventário → identifica brechas.
2. Critérios de investimento → priorizam locais mais vulneráveis.
3. Adequação → reduz risco de paralisações.

Responsável: CODAT

Situação: Não Iniciado

KRI: % de unidades sem redundância mínima de rede no trimestre.

Interpretação do KRI: Indicador direto do risco de interrupção dos serviços.

Fórmula: KRI= (Unidades sem redundância mínima / Total de unidades) ×100

Meta: ≤ 5%

3.4.4 Risco: R64 – ID: CPROD-04 – Estoque mínimo cobre apenas demandas ordinárias, comprometendo resposta a demandas extraordinárias

Tipo de Risco: Operacional

O estoque mínimo atual de equipamentos de infraestrutura (servidores, peças, módulos etc.) não suporta demandas extraordinárias, podendo atrasar projetos, atualizações e substituições emergenciais.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Integrar planejamento da demanda com Escritório de Projetos.
2. Criar política de dimensionamento de estoque mínimo por categoria.
3. Criar alertas automáticos de consumo.
4. Atualizar estoque considerando projetos futuros.

Como cada ação reduz o risco

1. Dimensionamento correto → reduz riscos de interrupções.
2. Alertas → evitam ruptura de estoque.

Responsável: CODAT

Situação: Planejado

KRI: % de consumo do estoque mínimo no mês.

Interpretação do KRI: Consumo elevado sinaliza risco de ruptura e indisponibilidade de reposição.

Fórmula: KRI= (Quantidade Consumida / Estoque Mínimo Definido) ×100

Meta: ≤ 70%

3.4.5 Risco: R65 – ID: CPROD-05 – Dispersão de documentos contratuais por número excessivo de sistemas e repositórios

Tipo de Risco: Operacional

Documentos estão armazenados em múltiplos repositórios, gerando inconsistência, risco de perda de informação, duplicidade e falhas na fiscalização de contratos.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Migrar documentos para sistema único;
2. Padronizar nomenclaturas e fluxos;
3. Formalizar revisão periódica;
4. Criar checklist de auditoria documental.

Como cada ação reduz o risco

1. Centralização → aumenta governança.
2. Checklists → garantem completude documental.

Responsável: CODAT

Situação: Não Iniciado

KRI: % de contratos centralizados em sistema único no mês.

Interpretação do KRI: Mede o nível de governança documental.

Fórmula: KRI= (Contratos centralizados/ Total de Contratos Ativos) ×100

Meta: ≥ 95%

3.4.6 Risco: R66 – ID: CPROD-06 – Licitações desertas por exigências excessivas em editais de TIC

Tipo de Risco: Operacional

Exigências técnicas excessivamente restritivas, cláusulas complexas ou mal estruturadas podem afastar fornecedores, resultando em licitações desertas, aumento de prazos, risco de descontinuidade de serviços críticos, necessidade de contratações emergenciais e impacto direto no planejamento de infraestrutura.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Revisar padrões de exigências técnicas dos editais para garantir proporcionalidade às necessidades.
2. Criar banco de lições aprendidas de licitações desertas anteriores.
3. Realizar consulta prévia ao mercado (market sounding) para validar exigências técnicas antes da publicação.
4. Criar checklist de conformidade técnica e jurídica para revisão dos TRs e editais.
5. Engajar áreas técnicas e SEPLAN para parecer conjunto que minimize riscos de restritividade excessiva.

Como cada ação reduz o risco

1. Revisão de exigências: amplia o número de fornecedores aptos.
2. Lições aprendidas: evita repetição de erros históricos.
3. Consulta prévia ao mercado: antecipa barreiras que levariam ao insucesso da licitação.
4. Checklist jurídico-técnico: aumenta qualidade e aderência legal dos editais.
5. Parecer conjunto: reduz risco de exigência mal fundamentada.

Responsável: CODAT

Situação: Não Iniciado

KRI: Taxa de licitações desertas da coordenação no trimestre.

Interpretação do KRI: Taxa elevada indica falhas no planejamento, restritividade excessiva e risco direto de descontinuidade de serviços essenciais.

Fórmula: KRI = (Número de licitações desertas ÷ Total de licitações realizadas no período) × 100

Meta: ≤ 5%

3.4.7 Risco: R67 – ID: CPROD-07 – Perda de dados e danos físicos por armazenamento inadequado de fitas de backup

Tipo de Risco: Operacional

Os backups ainda dependem de fitas magnéticas armazenadas sem controles robustos de segurança, sujeitas a danos físicos, incêndio, umidade, extravio, violação ou degradação física da mídia, o que pode resultar em perda irrecuperável de dados históricos, afetando sistemas judiciais, fiscais e administrativos.

Tipo de Tratamento: Controles Compensatórios

Plano de Tratamento

1. Decidir institucionalmente sobre a continuidade ou desativação progressiva do uso de fitas como mídia primária.
2. Criar inventário completo das fitas (local, conteúdo, data, criticidade, ciclo de retenção).
3. Adquirir cofres antichama e anti-umidade para armazenamento.
4. Criar processo formal de transporte seguro, com registro de retirada e devolução.
5. Avaliar alternativas de backup moderno (backup em nuvem ou armazenamento replicado).

Como cada ação reduz o risco

1. Decisão estratégica: elimina dependência de tecnologia obsoleta.
2. Inventário: garante rastreabilidade e reduz risco de perda.
3. Cofres seguros: reduzem probabilidade de dano físico.
4. Transporte controlado: mitiga risco de extravio.
5. Backup moderno: reduz dependência de mídias frágeis.

Responsável: CODAT

Situação: Planejado

KRI: Percentual de dados críticos armazenados exclusivamente em fitas no mês.

Interpretação do KRI: Quanto maior o percentual, maior o risco de perda ou indisponibilidade em caso de falha.

Fórmula: KRI = (Dados críticos que estão somente em fita ÷ Total de dados críticos) × 100

Meta: ≤ 10%

3.4.8 Risco: R68 – ID: CPROD-08 – Falhas de rede por switches críticos operando sem garantia ou suporte ativo

Tipo de Risco: Operacional

Switches de backbone e distribuição essenciais para a comunicação interna da rede institucional estão sem garantia ou sem contrato ativo, expondo o TJBA a falhas críticas de rede, paralisações, degradação e interrupções imprevistas.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Mapear todos os switches classificados como críticos.
2. Identificar switches sem garantia e classificá-los por grau de criticidade.
3. Definir plano de substituição escalonada, priorizando ambientes de maior risco.
4. Integrar controle de garantia ao inventário institucional.
5. Solicitar reforço orçamentário caso necessário.

Como cada ação reduz o risco

1. Mapeamento: revela o real nível de exposição.
2. Prioridade por criticidade: garante foco nos pontos de maior impacto.
3. Substituição escalonada: reduz risco progressivamente de forma factível.
4. Inventário atualizado: evita perda de prazo de garantia.

Responsável: CODAT

Situação: Planejado

KRI: % de switches críticos sem garantia ativa no trimestre.

Interpretação do KRI: Indica vulnerabilidade direta à falha abrupta sem suporte.

Fórmula: KRI = (Número de switches críticos sem garantia ÷ Total de switches críticos) × 100

Meta: ≤ 10%

3.4.9 Risco: R69 – ID: CPROD-09 – Sobrecarga da equipe por limitações de capacidade produtiva diante do aumento de demandas

Tipo de Risco: Operacional

A equipe técnica de produção e datacenter opera no limite da capacidade. O aumento das demandas sem reforço proporcional gera gargalos, erros, retrabalho, atrasos, riscos operacionais e incapacidade de atender necessidades críticas da SETIM.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Reportar a limitação de capacidade produtiva à governança para tomada de decisão estrutural.
2. Criar matriz de priorização de demandas por criticidade.
3. Formalizar processo de Gestão do Conhecimento da Produção para reduzir dependência individual.
4. Avaliar necessidade de contratação/reforço de equipe.
5. Criar indicadores de capacidade × demanda.

Como cada ação reduz o risco

1. Reporte à governança: viabiliza decisões sobre reforço ou reestruturação.
2. Priorização por criticidade: evita colapso das demandas essenciais.
3. Gestão do conhecimento: reduz dependência de pessoas-chave.
4. Reforço de equipe: corrige gargalos estruturais.
5. Indicadores: permitem controle e reação precoce.

Responsável: CODAT

Situação: Planejado

KRI: Índice de capacidade produtiva (demanda ÷ capacidade).

Interpretação do KRI: Indice superior a 1 indica saturação; acima de 0,85 já representa atenção crítica.

Fórmula: KRI = (Total de demandas recebidas no período ÷ Capacidade produtiva real no mesmo período)

Meta: ≤ 0,85

4 Diretoria de Sistemas de Informação (DIS)

A Diretoria de Sistemas de Informação (DIS) desempenha papel estratégico e central na transformação digital do Tribunal de Justiça da Bahia. É responsável por projetar, desenvolver, implantar, integrar e manter todos os sistemas judiciais e administrativos que suportam as atividades essenciais do TJBA, incluindo plataformas processuais, sistemas corporativos, integrações nacionais do CNJ, soluções analíticas e iniciativas emergentes baseadas em dados e Inteligência Artificial.

A atuação da DIS está diretamente relacionada à eficiência do serviço jurisdicional, à qualidade da experiência digital dos usuários internos e externos, à interoperabilidade com plataformas nacionais e à modernização contínua dos fluxos de trabalho. Em um ecossistema tecnológico cada vez mais complexo e integrado, a DIS assume a responsabilidade de garantir que sistemas críticos operem de forma estável, padronizada, segura e aderente às diretrizes nacionais como ENTIC-JUD, Resoluções do CNJ, políticas de segurança e parâmetros de governança digital.

Os riscos da DIS revelam a importância de não apenas como área técnica, mas como vetor estratégico para a execução do PDTIC, assegurar o cumprimento das metas institucionais e evolução do ecossistema digital do Tribunal.

Como guardiã dos sistemas, dados, integrações e jornadas digitais, a DIS sustenta a continuidade da justiça eletrônica, reduz riscos institucionais e acelera a modernização tecnológica do TJBA.

4.1 Plano de Tratamento dos Riscos da Diretoria de Sistemas de Informação (DIS):

A Diretoria de Sistemas (DIS) é responsável por garantir a integração, confiabilidade, evolução, segurança e interoperabilidade dos sistemas judiciais e administrativos do Tribunal de Justiça da Bahia.

Sua atuação é estratégica, pois sustenta plataformas críticas como sistemas processuais eletrônicos, sistemas administrativos, APIs institucionais, fluxos de interoperabilidade nacional, automações, integrações e governança de dados/IA.

Os riscos mapeados na DIS evidenciam desafios estruturais que impactam diretamente a eficácia da transformação digital do TJBA, tais como:

Principais riscos mapeados (executivo):

- Falhas de interoperabilidade nacional por arquitetura pouco modular, dificultando integração com CNJ e tribunais parceiros.
- Cobertura incompleta dos sistemas eletrônicos, com risco de descumprimento de metas estratégicas.
- Governança incipiente de Inteligência Artificial, com risco extremo de vieses, erros e responsabilização institucional.
- Integrações administrativas parciais, gerando retrabalho, inconsistências e controles manuais.

4.1.1 Risco: R70 – ID: DIS-01 – Não conformidade regulatória por arquitetura pouco modular e baixa aderência a padrões nacionais de interoperabilidade

Tipo de Risco: Estratégico

A arquitetura atual dos sistemas do TJBA possui baixa modularidade e falta de aderência aos padrões nacionais (CNJ, ENTIC-JUD, ICP-OAB), dificultando interoperabilidade com outros tribunais, barramento nacional, APIs padrão e integrações necessárias à Justiça 4.0.

Isso gera risco de não conformidade regulatória, retrabalho, atraso em integrações e perda de eficiência institucional.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Formalizar framework de integração nacional alinhado ao CNJ.
2. Criar catálogo institucional único de APIs, centralizado e documentado.
3. Priorizar refatoração de integrações críticas (integrações PJe, BNMP, SNIP, SEEU etc.).
4. Estabelecer arquitetura alvo com componentização e desacoplamento.
5. Criar checklist de aderência a padrões nacionais para novos sistemas.
6. Implementar periodicidade de revisão das integrações existentes.

Como cada ação reduz o risco

1. Framework nacional → garante conformidade regulatória contínua.
2. Catálogo único de APIs → reduz duplicidades e erros de integração.
3. Refatoração de integrações críticas → diminui falhas operacionais.
4. Arquitetura modular → aumenta escalabilidade e reduz retrabalho.
5. Checklists → evitam que novos sistemas nasçam fora do padrão.

Responsável: DIS

Situação: Planejado

KRI: Percentual de integrações críticas aderentes ao padrão nacional no trimestre.

Interpretação do KRI: Quanto menor o percentual, maior o risco de não conformidade, falhas em integrações, retrabalho e penalizações regulatórias do CNJ.

Fórmula: KRI = (Número de integrações críticas aderentes ao padrão ÷ Total de integrações críticas mapeadas) × 100

Meta: ≥ 95%

4.1.2 Risco: R71 – ID: DIS-02 – Cobertura incompleta dos sistemas eletrônicos nas unidades judiciais, com risco de descumprimento de metas estratégicas do TJBA

Tipo de Risco: Estratégico

A migração e adoção dos sistemas judiciais eletrônicos ainda ocorre de forma desigual nas comarcas, causando inconsistência operacional, retrabalho, experiência digital irregular e risco de descumprimento das metas do CNJ e do planejamento estratégico do TJBA.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Mapear cobertura atual sistema × comarca.
2. Criar ondas de migração com cronograma e apoio de treinamento.
3. Restringir novas evoluções em sistemas legados.
4. Criar painéis de migração para diretoria.
5. Implementar governança de adoção de sistemas.
6. Estabelecer comunicação contínua com magistrados e unidade.

Como cada ação reduz o risco

1. Migração planejada → reduz atrasos.
2. Painéis → aumentam visibilidade.
3. Restrição de legados → evita efeito “dual stack”.
4. Governança → padroniza processos e acelera adoção.

Responsável: DIS

Situação: Planejado

KRI: Percentual de unidades judiciais operando no sistema eletrônico padrão no mês.

Interpretação do KRI: Baixa adoção indica risco direto de descumprimento das metas estratégicas e inconsistência entre unidades.

Fórmula: KRI = (Unidades judiciais operando no sistema padrão ÷ Total de unidades judiciais) × 100

Meta: ≥ 90% até fim de 2026

4.1.3 Risco: R72 – ID: DIS-03 – Risco extremo de vieses, erros e uso indevido de Inteligência Artificial por ausência de governança formal de IA

Tipo de Risco: Estratégico

A Diretoria DIS ainda não possui um modelo formal de governança de IA, inventário de modelos, processo de validação, monitoramento de vieses e trilha de auditoria.

Tipo de Tratamento: Controles Detectivos e Preventivos

Plano de Tratamento

1. Aprovar e publicar Política de IA Responsável do TJBA.
2. Criar inventário oficial de modelos de IA em uso e em desenvolvimento.
3. Implantar processo de avaliação, testes e validação técnica-jurídica.
4. Criar trilha de auditoria permanente de IA.

5. Estabelecer indicadores de governança e mecanismos de acompanhamento.
6. Integrar governança de IA à CGTIC e ao Comitê de Segurança.

Como cada ação reduz o risco

1. Política → cria base normativa.
2. Inventário → garante visibilidade e controle.
3. Avaliação/testes → reduz vieses e erros sistêmicos.
4. Auditoria → aumenta accountability.
5. Comitê → eleva a maturidade e integração entre áreas.

Responsável: DIS

Situação: Em Execução

KRI: Percentual de soluções de IA com governança formal implantada no trimestre.

Interpretação do KRI: Indica maturidade da governança de IA. Baixa adesão representa risco extremo de erros e responsabilização institucional.

Fórmula: KRI = (Soluções de IA com governança formal ÷ Total de soluções de IA identificadas) × 100

Meta: ≥ 90%

4.1.4 Risco: R73 – ID: DIS-04 – Ineficiência e inconsistência operacional por integrações parciais entre sistemas administrativos

Tipo de Risco: Estratégico

As integrações entre os sistemas administrativos do TJBA ainda apresentam lacunas, controles manuais, duplicidade de cadastros e fluxos paralelos, gerando retrabalho, inconsistências e fragilidade nos controles internos.

Tipo de Tratamento: Controles Detectivos e Compensatório

Plano de Tratamento

1. Priorizar integrações críticas entre SEI, ERP-RH e NAF.
2. Mapear e eliminar controles manuais paralelos.
3. Criar plano diretor de integrações administrativas.
4. Instituir governança de integrações com padrões claros.
5. Padronizar tabelas-mestras institucionais.
6. Criar indicadores de aderência à integração.

Como cada ação reduz o risco

1. Integrações críticas → reduzem inconsistências.
2. Eliminação de controles manuais → reduz falhas humanas.
3. Governança → impede criação de sistemas paralelos.
4. Padronização → aumenta qualidade e integridade de dados.

Responsável: DIS

Situação: Planejado

KRI: Percentual de processos administrativos críticos sem necessidade de controles manuais no trimestre.

Interpretação do KRI: Quanto maior o percentual de processos totalmente integrados, maior a eficiência e menor o risco de erros.

Fórmula: KRI = (Processos críticos sem controles manuais ÷ Total de processos administrativos críticos) × 100

Meta: ≥ 80%

4.2 Plano de Tratamento dos Riscos da Coordenação de Sistemas Judiciais (CSJUD):

A CSJUD é responsável por toda a sustentação, evolução, qualidade e governança técnica dos sistemas judiciais eletrônicos do TJBA, incluindo PJe, ePROC, SEEU, BNMP, sistemas de consulta, integrações CNJ e sistemas satélites que suportam fluxos jurisdicionais e de magistrados.

A coordenação atua em um ambiente altamente crítico, pois qualquer falha nos sistemas judiciais afeta diretamente o funcionamento da Justiça, a produtividade de magistrados e servidores, e indicadores oficiais do CNJ.

Os riscos mapeados refletem problemas que impactam diretamente a disponibilidade, qualidade, segurança, automação, processos de QA, conectividade e consistência de ambientes, como:

- Falhas e vulnerabilidades devido à baixa capacidade de QA/observabilidade.
- Dependência de pessoas chave e padrões não unificados nas automações judiciais.
- Riscos contratuais (TRs, saldos de contrato, priorização de demandas externas).
- Falhas de requisitos e retrabalho por documentação incompleta.
- Divergências entre ambientes (DEV/HML/PRD) que geram incidentes em produção.

4.2.1 Risco: R74 – ID: CSJUD-01 – Falhas, indisponibilidade ou vulnerabilidades nos serviços judiciais digitais por falta de observabilidade e testes adequados

Tipo de Risco: Operacional

A ausência de observabilidade técnica (logs estruturados, métricas, telemetria) e de testes adequados (QA contínuo, testes automatizados) nos sistemas judiciais digitais gera risco de falhas não detectadas, degradação de desempenho e indisponibilidade dos serviços essenciais (PJe, ePROC, BNMP, SEEU etc.).

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implantar observabilidade plena: logs estruturados, métricas, telemetria e tracing distribuído.
2. Criar e aplicar pipeline permanente de QA com cobertura mínima pactuada.

3. Desenvolver testes automatizados de regressão para fluxos judiciais críticos.
4. Criar painel executivo de estabilidade para a DIS/CSJUD.
5. Definir SLAs de detecção de incidentes e gatilhos de escala.

Como cada ação reduz o risco

1. Observabilidade detecta falhas rapidamente.
2. Testes automatizados evitam regressões.
3. QA contínuo melhora a estabilidade técnica.

Responsável: CSJUD

Situação: Planejado

KRI: % de integrações judiciais críticas com observabilidade completa por mês.

Interpretação do KRI: monitora o nível de controle técnico e a existência de valores baixos indicam risco de incidentes invisíveis.

Fórmula: KRI = (Integrações críticas com observabilidade completa ÷ Total de integrações críticas) × 100

Meta: ≥ 95%

4.2.2 Risco: R75 – ID: CSJUD-02 – Falhas nas automações judiciais por ausência de padrões técnicos, documentação e dependência de pessoas chave

Tipo de Risco: Tático

Automatizações judiciais (RPA, scripts, fluxos automatizados) não seguem padrões unificados, não possuem documentação adequada e dependem de pessoas específicas, aumentando risco de falhas emergenciais, indisponibilidades e incapacidade de manutenção.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar padrão institucional de automações (arquitetura, logs, nomenclatura).
2. Criar repositório central versionado com controle de acesso.
3. Documentar todas as automações críticas.
4. Implantar pair programming e tutoria para reduzir dependências individuais.
5. Revisar automações por criticidade e impacto.

Como cada ação reduz o risco

1. Padronização → reduz falhas e aumenta previsibilidade.
2. Documentação → garante continuidade.
3. Repositório central → evita perda de código.
4. Tutoria → reduz dependência de pessoas-chave.

Responsável: CSJUD

Situação: Em Execução

KRI: % de automações judiciais padronizadas e documentadas por semestre.

Interpretação do KRI: valores baixos indicam risco alto de falhas e indisponibilidade.

Fórmula: KRI = (Automações padronizadas e documentadas ÷ Total de automações judiciais) × 100

Meta: ≥ 70% (em 2 anos)

4.2.3 Risco: R76 – ID: CSJUD-03 – Atrasos, erros ou impugnações em TRs judiciais por falhas técnicas ou omissões nos requisitos

Tipo de Risco: Operacional

Termos de Referência judiciais têm apresentado erros, falhas de requisitos e ausência de validação cross-área, aumentando risco de impugnações, atrasos e falhas na contratação de serviços essenciais.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar checklist técnico padronizado de TR judicial.
2. Criar repositório de modelos validados.
3. Aplicar revisão cruzada CSJUD × DIS × CGTIC.
4. Registrar lições aprendidas de certames anteriores.

Como cada ação reduz o risco

1. Checklist → reduz omissões técnicas.
2. Revisão cruzada → aumenta qualidade.
3. Modelos padrão → evita erros recorrentes.

Responsável: CSJUD

Situação: Planejado

KRI: % de TRs judiciais devolvidos por inconsistência técnica por trimestre.

Interpretação do KRI: indicador direto de maturidade do processo de contratação.

Fórmula: KRI = (TRs devolvidos por inconsistência ÷ Total de TRs enviados) × 100

Meta: ≤ 5%

4.2.4 Risco: R77 – ID: CSJUD-04 – Saldo contratual insuficiente por aumento de demanda ou falha de previsão

Tipo de Risco: Operacional

Demandas judiciais crescentes podem consumir rapidamente o saldo contratual, causando atrasos, retração da capacidade de entrega e risco de paralisação.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar painel de consumo contratual (curto/médio prazo).
2. Criar premissas de previsão de saldo × demanda × capacidade.
3. Implantar monitoramento mensal de consumo.
4. Criar gatilhos para solicitação de aditivo.

Como cada ação reduz o risco

1. Previsibilidade → evita ruptura contratual.
2. Gatilhos → corrigem desvios antes de impacto crítico.

Responsável: CSJUD

Situação: Em Execução

KRI: % de contratos judiciais com saldo projetado insuficiente no mês.

Interpretação do KRI: monitora risco de interrupção de serviços contratados.

Fórmula: KRI = (Contratos com saldo projetado insuficiente ÷ Total de contratos judiciais) × 100

Meta: ≤ 10%

4.2.5 Risco: R78 – ID: CSJUD-05 – Perda de prazo, atraso e retrabalho por picos de demandas judiciais e sobrecarga operacional

Tipo de Risco: Operacional

O aumento de demandas judiciais em determinados ciclos, associado à limitação de capacidade da equipe técnica, provoca acúmulo de tarefas, atrasos, retrabalho, perda de qualidade nas entregas e risco de descumprimento de solicitações judiciais prioritárias.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Revisar semestralmente o plano de demandas da CSJUD.
2. Utilizar contratos com capacidade elástica para absorver picos.
3. Criar consideração de impacto por tipo de demanda (criticidade × urgência).
4. Criar painel gerencial de demanda vs. capacidade, compartilhado com DIS.
5. Criar fluxos formais para redistribuição temporária de equipe em situações de pico.

Como cada ação reduz o risco

1. Revisões periódicas → ajustam capacidade antes do colapso.
2. Contratos elásticos → absorvem picos de forma rápida e previsível.
3. Painéis → permitem decisões de priorização mais ágeis.
4. Redistribuição de equipe → diminui gargalos técnicos imediatos.

Responsável: CSJUD

Situação: Não Iniciado

KRI: % de demandas judiciais rejeitadas ou devolvidas por falta de capacidade por trimestre.

Interpretação do KRI: Valores altos indicam desequilíbrio entre demanda e capacidade, aumentando risco operacional.

Fórmula: KRI = (Demandas rejeitadas ou devolvidas ÷ Total de demandas judiciais recebidas) × 100

Meta: ≤ 15%

4.2.6 Risco: R79 – ID: CSJUD-06 – Falhas, atrasos e inconsistências por ausência de critérios formais de priorização das demandas judiciais

Tipo de Risco: Operacional

Demandas judiciais são priorizadas informalmente, sem critérios institucionais claros, gerando atrasos, tratamento desigual das solicitações, conflitos de prioridade e riscos de impacto em processos críticos.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar matriz institucional de priorização, considerando impacto judicial, criticidade, urgência, valor público e risco regulatório.
2. Publicar backlog priorizado para transparência interna.
3. Criar acordos de capacidade (capacity agreements) com DIS e superintendências.
4. Incluir critério de priorização no fluxo do sistema de gestão de demandas.
5. Monitorar periodicamente pedidos urgentes × prioridades definidas.

Como cada ação reduz o risco

1. Critérios claros → reduzem conflitos internos.
2. Backlog visível → aumenta transparência.
3. Acordos de capacidade → evitam priorizações ad hoc.

Responsável: CSJUD

Situação: Planejado

KRI: Indicador: % de demandas judiciais atrasadas por ausência de priorização definida por mês.

Interpretação do KRI: Percentuais altos significam falha na governança e risco direto às entregas judiciais.

Fórmula: KRI = (Demandas atrasadas sem priorização clara ÷ Total de demandas judiciais em andamento) × 100

Meta: ≤ 10%

4.2.7 Risco: R80 – ID: CSJUD-07 – Vulnerabilidades críticas e falhas em produção por testes insuficientes e ausência de QA formal

Tipo de Risco: Operacional

Aplicações judiciais apresentam testes insuficientes, ausência de testes de regressão, baixa automatização e inconsistências entre versões, resultando em incidentes graves em produção, indisponibilidades e erros funcionais.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implantar teste de carga, estresse e regressão para sistemas judiciais críticos.
2. Implantar pipeline CI/CD com gatilhos de QA obrigatório.
3. Criar política institucional de testes mínimos obrigatórios (coverage baseline).
4. Mapear riscos funcionais críticos e criar cenários automatizados.
5. Implementar ambiente de homologação sincronizado com PRD.

Como cada ação reduz o risco

1. Testes robustos → reduzem falhas em produção.
2. QA integrado ao CI/CD → evita releases sem validação.
3. Cenários automatizados → reduzem regressões funcionais.
4. HML sincronizado → reduz divergências ambientai.

Responsável: CSJUD

Situação: Não Iniciado

KRI: % de releases judiciais submetidos ao QA completo por mês.

Interpretação do KRI: Quanto menor o número, maior a chance de falhas em produção.

Fórmula: KRI = (Releases submetidos ao QA completo ÷ Total de releases realizados) × 100

Meta: ≥ 95%

4.2.8 Risco: R81 – ID: CSJUD-08 – Falhas técnicas e retrabalho por documentação insuficiente dos sistemas judiciais

Tipo de Risco: Operacional

A documentação dos sistemas judiciais é incompleta ou desatualizada, causando retrabalho, dependência de pessoas chave, lentidão em manutenção, erros recorrentes e dificuldade para evolução técnica.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar repositório único para documentação dos sistemas.
2. Definir documentação mínima obrigatória por sistema (arquitetura, APIs, fluxos).

3. Criar ciclo de revisão semestral de documentação.
4. Implementar auditoria com checklist de integridade documental.
5. Integrar documentação à base de conhecimento da DIS.

Como cada ação reduz o risco

1. Padronização → reduz retrabalho.
2. Checklist → garante completude.
3. Revisões periódicas → evita obsolescência.
4. Repositório único → reduz perda de conhecimento.

Responsável: CSJUD

Situação: Planejado

KRI: % de sistemas judiciais com documentação atualizada a cada semestre.

Interpretação do KRI: Baixa documentação indica risco elevado de falhas, lentidão e dependência de indivíduos.

Fórmula: KRI = (Sistemas judiciais com documentação atualizada ÷ Total de sistemas judiciais mapeados) × 100

Meta: ≥ 80%

4.2.9 Risco: R82 – ID: CSJUD-09 – Retrabalho e atrasos por falhas de requisitos judiciais

Tipo de Risco: Operacional

Falhas na definição de requisitos judiciais provocam retrabalho, atrasos, inconsistências funcionais e baixa qualidade das entregas, afetando diretamente o fluxo jurisdicional.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar templates padronizados de requisitos.
2. Realizar workshops de requisitos com usuários judiciais.
3. Criar validação cruzada CSJUD × magistrados × DIS.
4. Criar banco de requisitos reutilizáveis para casos semelhantes.

Como cada ação reduz o risco

1. Templates → reduzem erros comuns.
2. Validação cruzada → melhora aderência funcional.
3. Banco de requisitos → reduz inconsistências.

Responsável: CSJUD

Situação: Planejado

KRI: % de entregas judiciais com retrabalho por falha de requisitos por mês.

Interpretação do KRI: Indica a maturidade da engenharia de requisitos.

Fórmula: KRI = (Entregas com retrabalho por falha de requisito ÷ Total de entregas judiciais) × 100

Meta: ≤ 15%

4.2.10 Risco: R83 – ID: CSJUD-10 – Incidentes em produção por divergências entre ambientes (DEV/HML/PRD)

Tipo de Risco: Operacional

Diferenças entre ambientes DEV, HML e PRD causam falhas, erros funcionais e incidentes em produção, especialmente quando há versões, configurações e bases diferentes entre ambientes..

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implantar pipeline CI/CD com versionamento unificado.
2. Implementar sincronização periódica HML ↔ PRD.
3. Criar checklist de deploy e validação de ambientes.
4. Criar política institucional de controle de alterações.
5. Criar indicadores de aderência entre ambientes.

Como cada ação reduz o risco

1. CI/CD → evita divergências de versão.
2. Sincronização → reduz inconsistências.
3. Checklists → garantem conformidade no deploy.

Responsável: CSJUD

Situação: Não Iniciado

KRI: % de incidentes judiciais originados por divergência entre ambientes por mês.

Interpretação do KRI: Alta incidência indica falha estrutural na governança técnica.

Fórmula: KRI = (Incidentes causados por divergência de ambiente ÷ Total de incidentes judiciais) × 100

Meta: ≤ 5%

4.3 Plano de Tratamento dos Riscos da Coordenação de Sistemas Administrativos (COSIS):

A COSIS é responsável pela gestão, sustentação, integração, evolução e qualidade dos sistemas administrativos corporativos do TJBA — como ERP de RH e Financeiro, SEI, NAF, sistemas satélites, automações administrativas, integrações intersistemas, dataflows e processos de apoio.

É uma área fundamental para a confiabilidade dos processos administrativos, garantindo governança de contratos, execução orçamentária, folha de pagamento,

suprimentos, patrimônio, processos de pessoal e comunicação com áreas finalísticas.

Os riscos mapeados mostram necessidades de controles e aprimoramentos em:

- QA insuficiente em sistemas administrativos críticos;
- Automação fragmentada e dependente de pessoas chave;
- Riscos contratuais e falhas de TRs;
- Saldos contratuais e capacidade produtiva;
- Processos sem critérios claros de priorização;
- Requisitos incompletos, retrabalho e falhas funcionais;
- Divergências entre ambientes DEV/HML/PRD.

4.3.1 Risco: R84 – ID: COSIS-01 – Vulnerabilidades, falhas e indisponibilidades em sistemas administrativos por testes insuficientes

Tipo de Risco: Operacional

Sistemas administrativos críticos (ERP RH, ERP Financeiro, SEI, NAF, etc.) possuem cobertura insuficiente de QA, ausência de testes automatizados e pouca visibilidade sobre falhas potenciais, resultando em risco de incidentes, erros funcionais, retrabalho e indisponibilidade de serviços.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Implantar política de QA administrativo com critérios mínimos de cobertura.
2. Criar conjunto de testes automatizados para rotinas essenciais.
3. Implantar observabilidade para módulos críticos (logs estruturados e métricas).
4. Criar pipeline CI/CD com validações obrigatórias de QA.
5. Realizar testes regressivos antes de cada release.

Como cada ação reduz o risco

1. QA estruturado diminui falhas em produção.
2. Observabilidade detecta problemas rapidamente.
3. Testes automatizados reduzem regressões funcionais.

Responsável: COSIS

Situação: Planejado

KRI: % de integrações administrativas críticas monitoradas por QA completo por mês.

Interpretação do KRI: Percentuais baixos indicam risco elevado de falhas funcionais não detectadas.

Fórmula: KRI = (Integrações críticas com QA completo ÷ Total de integrações críticas) × 100

Meta: ≥ 95%

4.3.2 Risco: R85 – ID: COSIS-02 – Falhas nas automações administrativas por padrões heterogêneos e dependência de pessoas chave

Tipo de Risco: Tático

Automatizações de processos administrativos usam padrões distintos, não possuem documentação mínima e dependem de técnicos específicos, gerando risco de falhas, interrupções e incapacidade de manutenção em casos de ausência/substituição.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar padrão institucional de automações administrativas.
2. Documentar automações críticas em repositório versionado.
3. Criar tutoria, rotatividade planejada e pair programming.
4. Criar auditoria anual das automações.
5. Priorizar automações de maior impacto.

Como cada ação reduz o risco

1. Padronização → reduz falhas.
2. Documentação → garante continuidade.
3. Auditoria → detecta fragilidades.

Responsável: COSIS

Situação: Planejado

KRI: % de automações padronizadas e documentadas por semestre.

Interpretação do KRI: Quanto menor o valor, maior o risco de indisponibilidade e falhas.

Fórmula: KRI = (Automações padronizadas/documentadas ÷ Total de automações administrativas) × 100

Meta: ≥ 70%

4.3.3 Risco: R86 – ID: COSIS-03 – Atrasos e inconsistências contratuais por falhas técnicas em TRs administrativos

Tipo de Risco: Operacional

Termos de Referência de sistemas administrativos têm sido devolvidos por inconsistências ou requisitos incompletos, gerando atrasos, retrabalho, risco de impugnação e impacto nos projetos dependentes.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar checklist técnico padronizado de TR administrativo.
2. Criar repositório de TRs-modelo institucional.
3. Realizar validação cruzada entre COSIS × DIS × CGTIC.

4. Coletar lições aprendidas em certames anteriores.

Como cada ação reduz o risco

1. Checklist → garante completude.
2. Revisão cruzada → aumenta acurácia técnica.
3. Modelos → reduzem erros básicos.

Responsável: COSIS

Situação: Planejado

KRI: % de TRs administrativos devolvidos por inconsistência técnica por trimestre.

Interpretação do KRI: Indicador direto da maturidade da produção de TR.

Fórmula: KRI = (TRs devolvidos por inconsistência ÷ Total de TRs emitidos) × 100

Meta: ≤ 5%

4.3.4 Risco: R87 – ID: COSIS-04 – Risco de esgotamento de saldo contratual por sobrecarga de demandas

Tipo de Risco: Operacional

Aumento de demandas administrativas sem previsão adequada pode comprometer o saldo dos contratos, gerando paralisação de entregas, necessidade de aditivos emergenciais e risco de atrasos estruturais.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar painel de consumo contratual.
2. Realizar projeção de saldo × demanda × capacidade.
3. Criar gatilhos de alerta para saldo crítico.
4. Criar plano de contingência para continuidade.

Como cada ação reduz o risco

1. Painéis → antecipam riscos de interrupção.
2. Gatilhos → permitem ação corretiva rápida.

Responsável: COSIS

Situação: Em Execução

KRI: % de contratos administrativos com saldo projetado insuficiente por mês.

Interpretação do KRI: Valores altos indicam risco de ruptura contratual.

Fórmula: KRI = (Contratos com saldo crítico projetado ÷ Total de contratos administrativos) × 100

Meta: ≤ 10%

4.3.5 Risco: R88 – ID: COSIS-05 – Atrasos e falhas por ausência de critérios formais de priorização de demandas administrativas

Tipo de Risco: Tático

Demandas administrativas chegam à COSIS de forma heterogênea, sem critérios institucionais claros para priorização, gerando atrasos, conflitos e alocação ineficiente de capacidade.

Tipo de Tratamento: Controles Detectivo e Compensatório

Plano de Tratamento

1. Criar matriz de priorização administrativa.
2. Publicar backlog priorizado para unidades.
3. Criar "acordos de capacidade" com coordenadores.
4. Configurar o sistema de demandas com critérios formais.

Como cada ação reduz o risco

1. Critérios claros → reduz conflitos.
2. Backlog transparente → racionaliza alocação.

Responsável: COSIS

Situação: Planejado

KRI: % de demandas administrativas atrasadas por ausência de priorização por mês.

Interpretação do KRI: Indica falha na governança de demandas.

Fórmula: KRI = (Demandas atrasadas por falta de priorização ÷ Total de demandas administrativas em andamento) × 100

Meta: ≤ 10%

4.3.6 Risco: R89 – ID: COSIS-06 – Retrabalho e falhas por requisitos administrativos incompletos ou mal definidos

Tipo de Risco: Operacional

Sistemas administrativos sofrem retrabalho significativo e erros funcionais devido à baixa qualidade dos requisitos, ausência de padrões e insuficiência de validação junto às áreas requisitantes.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar templates padronizados de requisitos.
2. Realizar workshops de requisitos com unidades administrativas.
3. Criar fase obrigatória de revisão técnico-funcional.
4. Implementar backlog de requisitos reutilizáveis.

Como cada ação reduz o risco

1. Templates → reduzem erros.

2. Workshops → aumentam precisão.
3. Validações → evitam retrabalho.

Responsável: COSIS

Situação: Não Iniciado

KRI: % de entregas administrativas com retrabalho por falha de requisitos por mês.

Interpretação do KRI: Baixa maturidade de engenharia de requisitos.

Fórmula: KRI = (Entregas com retrabalho por falha de requisito ÷ Total de entregas administrativas) × 100

Meta: ≤ 15%

4.3.7 Risco: R90 – ID: COSIS-07 – Falhas e inconsistências por ausência de QA formal nas automações administrativas

Tipo de Risco: Operacional

Automações administrativas (RPA, rotinas automatizadas, scripts) são implantadas sem QA robusto, criando risco de execução incorreta, falhas silenciosas e degradação de processos administrativos essenciais.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar política de QA para automações administrativas.
2. Desenvolver testes automatizados para rotinas críticas.
3. Registrar logs detalhados e indicadores de integridade.
4. Criar auditoria trimestral de automações.

Como cada ação reduz o risco

1. QA → aumenta confiabilidade técnica.
2. Logs → permitem rastrear falhas.
3. Auditorias → detectam erros ocultos.

Responsável: COSIS

Situação: Planejado

KRI: % de automações administrativas submetidas ao QA completo por mês.

Interpretação do KRI: Valores baixos indicam alta exposição a falhas automatizadas.

Fórmula: KRI = (Automações com QA completo ÷ Total de automações administrativas) × 100

Meta: ≥ 90%

4.3.8 Risco: R91 – ID: COSIS-08 – Incidentes e falhas devido a divergências entre ambientes DEV/HML/PRD

Tipo de Risco: Operacional

Diferenças entre configurações, versões e dados entre DEV, HML e PRD resultam em falhas ao implantar releases, causando incidentes, retrabalho e indisponibilidade de sistemas administrativos.

Tipo de Tratamento: Controles Detectivo e Corretivo

Plano de Tratamento

1. Criar pipeline CI/CD com versionamento único.
2. Sincronizar HML e PRD periodicamente.
3. Criar checklist obrigatório de deploy.
4. Criar política institucional de controle de alterações.

Como cada ação reduz o risco

1. CI/CD → reduz diferenças de versão.
2. Sincronização → evita divergências funcionais.
3. Checklists → aumentam confiabilidade operacional.

Responsável: COSIS

Situação: Não Iniciado

KRI: % de incidentes administrativos causados por divergência de ambiente por mês.

Interpretação do KRI: Quanto maior o percentual, maior será a fragilidade da governança técnica.

Fórmula: KRI = (Incidentes por divergência de ambiente ÷ Total de incidentes administrativos) × 100

Meta: ≤ 5%

5 Assessoria de Segurança da Informação (ASI)

A Assesoria de Segurança da Informação (ASI) tem papel estratégico na proteção dos ativos de informação do Tribunal, incluindo dados processuais, dados pessoais de magistrados, servidores e jurisdicionados, bem como a infraestrutura tecnológica que sustenta os serviços judiciais e administrativos. Em um contexto de transformação digital, alta dependência de sistemas críticos e exigências regulatórias como a LGPD e as normas do CNJ, a ASI atua como guardiã da confidencialidade, integridade, disponibilidade e autenticidade da informação, alinhando-se às diretrizes de gestão de riscos previstas na ABNT NBR ISO 31000, no COSO ERM e nas boas práticas de segurança (ISO/IEC 27001, 27002 e 27701).

O Comitê Gestor de Segurança da Informação (CGSI) exerce função de instância colegiada de governança, definindo diretrizes, priorizando iniciativas e acompanhando os principais indicadores de risco de SI. Na prática, é no CGSI que se alinham as estratégias de proteção da informação com os objetivos institucionais, garantindo que as decisões de segurança estejam integradas ao planejamento de TIC e ao Plano de Transformação Digital do Tribunal. Cabe ao CGSI apoiar a alta administração na definição do apetite a risco em SI, aprovar políticas e normas e demandar planos de tratamento para riscos inaceitáveis.

O Núcleo de Segurança da Informação (NSI), por sua vez, atua de forma mais tática e operacional, sendo responsável por implementar controles, monitorar eventos de segurança, tratar incidentes, apoiar projetos de TIC com análises de risco e garantir a aderência às políticas aprovadas pelo CGSI. É o NSI que faz a “ponte” entre as diretrizes de governança e a realidade técnica, participando do ciclo de vida de sistemas, avaliando fornecedores, parametrizando ferramentas (firewalls, SIEM, antivírus, DLP, IAM/IGA etc.) e mantendo evidências para auditorias internas e externas.

Em conjunto, ASI, CGSI e NSI estruturam a Gestão de Riscos de Segurança da Informação no Tribunal, sendo que a ASI coordena a visão integrada de riscos de SI, consolidando matrizes de risco, propondo planos de tratamento e monitorando KRIs, o CGSI assegura o alinhamento com a estratégia institucional e com as normas do CNJ, priorizando recursos e decisões de alto impacto e o NSI implementa e opera controles técnicos e processos de segurança, garantindo que as ações previstas nos planos de tratamento sejam efetivamente executadas e monitoradas.

Esse modelo fortalece a responsabilização, a transparência e a conformidade regulatória, ao mesmo tempo em que reduz a probabilidade e o impacto de eventos que poderiam comprometer a continuidade dos serviços judiciais, a confiança da sociedade e a imagem institucional.

5.1 Plano de Tratamento dos Riscos da Assessoria de Segurança da Informação (ASI):

Os riscos de Segurança da Informação mapeados, em geral, se organizam em alguns grandes blocos temáticos, que são endereçados por planos de tratamento específicos:

- **Riscos de vazamento e uso indevido de dados pessoais e sensíveis**: Envolvem o acesso indevido a bases processuais, sistemas administrativos e repositórios de documentos, com potencial de violar a LGPD, gerar danos à imagem institucional e impactar a confiança da sociedade. Os planos de ação costumam incluir: controles de acesso mais granulares, revisão de perfis, trilhas de auditoria, criptografia, classificação da informação e reforço de políticas de uso aceitável.
- **Riscos de indisponibilidade de serviços essenciais por ataques cibernéticos (ransomware, DDoS, exploração de vulnerabilidades):** A indisponibilidade de sistemas processuais, portais e serviços ao jurisdicionado compromete diretamente a prestação jurisdicional. Os tratamentos típicos incluem: fortalecimento de backup e recuperação de desastres, testes de restauração, segmentação de rede, hardening de servidores, atualização contínua de patches e planos de continuidade de TIC integrados ao Plano de Continuidade de Negócios.
- **Riscos associados a terceiros, nuvem e soluções SaaS**: A crescente adoção de serviços em nuvem e soluções SaaS traz riscos de dependência tecnológica, falhas de configuração (misconfiguration) e não conformidade com requisitos de segurança contratual e regulatória. O tratamento passa por: cláusulas contratuais de segurança, due diligence de fornecedores, validação de arquitetura, governança de identidade e configuração segura em ambientes de nuvem.
- **Riscos de engenharia social, phishing e erro humano**: Usuários continuam sendo um vetor crítico de risco. A baixa conscientização em SI aumenta a probabilidade de incidentes, vazamentos e comprometimento de credenciais. Os planos de tratamento contemplam campanhas estruturadas de conscientização, simulações de phishing, reforço de políticas, treinamentos segmentados por perfil e uso de múltiplas camadas de autenticação (MFA, IGA, ZTNA).
- **Riscos de governança e mudança não controlada em serviços e sistemas**: Mudanças em produção sem análise de risco de SI podem introduzir vulnerabilidades, abrir portas para ataques ou gerar inconsistências de dados. O tratamento envolve: fortalecimento do processo de gestão de mudanças (change management), exigência de parecer de SI em mudanças críticas, esteira de desenvolvimento segura (DevSecOps) e integração da avaliação de risco no ciclo de vida de projetos.
- **Riscos de baixa visibilidade e monitoramento insuficiente (logs, SOC, detecção de incidentes**): Mesmo com controles implementados, se não houver monitoramento adequado, incidentes podem ficar “ocultos” por longos períodos. Os planos incluem a estruturação de um SOC (interno ou terceirizado), consolidação de logs, uso de SIEM, definição de casos de uso de monitoramento, playbooks de resposta a incidentes e melhoria da

integração entre NSI, equipes de infraestrutura, desenvolvimento e apoio ao usuário.

De forma geral, o Plano de Ação de Tratamento da ASI busca reduzir a probabilidade e o impacto desses grupos de risco por meio de uma combinação de:

- Controles técnicos (ferramentas, arquitetura, autenticação, criptografia, monitoramento);
- Controles organizacionais (políticas, normas, procedimentos, governança de mudanças);
- Controles humanos (conscientização, treinamento, responsabilização e cultura de segurança);
- Controles contratuais e de terceiros (SLAs, cláusulas de segurança, auditoria de fornecedores).

Os KRIs de Segurança da Informação associados a esses riscos permitem ao CGSI, à ASI e ao NSI acompanhar se os planos de tratamento estão surtindo efeito, sustentando decisões sobre prioridades, investimentos e eventuais revisões de apetite a risco.

5.1.1 Risco: R21 – ID: ASI-01 – Vazamento massivo ou Acesso indevido externo de Dados pessoais e sensíveis do TJBA por Fragilidade dos controles tecnológicos de privacidade

Tipo de Risco: Estratégico

Trata-se do risco de que dados pessoais e sensíveis sob responsabilidade do TJBA sejam expostos ou acessados indevidamente por agentes externos devido a fragilidades em controles tecnológicos de privacidade (por exemplo, ausência de criptografia adequada, DLP, controles de consentimento e minimização). A materialização desse risco gera danos reputacionais, pressão institucional, questionamentos regulatórios (LGPD) e perda de confiança da sociedade.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Criar inventário de controles de privacidade aplicáveis aos sistemas e bases de dados pessoais e sensíveis.
2. Implementar indicadores de aderência tecnológica à LGPD (ex.: criptografia, pseudonimização, trilhas de auditoria).
3. Ampliar a automação de controles técnicos de privacidade (criptografia, DLP, consentimento, minimização de dados).

Como cada ação reduz o risco

1. O inventário de controles de privacidade dá visibilidade sobre o que efetivamente protege os dados hoje, permitindo identificar lacunas e priorizar correções, reduzindo a probabilidade de vazamentos por ausência de controle.
2. Os indicadores de aderência tecnológica à LGPD permitem acompanhar, em nível de gestão, o quanto os sistemas estão alinhados aos requisitos de proteção de dados, facilitando decisões sobre investimentos e correções antes que um incidente grave ocorra.
3. A automação de controles técnicos (criptografia, DLP, consentimento, minimização) reduz dependência de procedimentos manuais e torna mais difícil que um atacante externo explore fragilidades, diminuindo tanto a probabilidade quanto o impacto de um vazamento massivo.

Responsável: ASI

Situação: Planejado

KRI: % de controles tecnológicos de privacidade implementados (Mensal).

Interpretação do KRI: Este KRI mede o percentual de controles tecnológicos de privacidade previstos (por exemplo, criptografia em repouso e em trânsito, DLP, mascaramento, logging de acesso, mecanismos de consentimento e minimização) que já estão efetivamente implementados. Quanto maior o percentual, maior a capacidade técnica do Tribunal de prevenir ou limitar vazamentos de dados pessoais. A evolução positiva do indicador, após a execução do plano de ação, evidencia redução da exposição ao risco de vazamento massivo e acesso indevido externo.

Fórmula: Percentual de controles tecnológicos de privacidade implementados = (Número de controles tecnológicos de privacidade

implementados / Número total de controles tecnológicos de privacidade previstos) × 100

Meta: ≥ 95%

5.1.2 Risco: R22 – ID: ASI-02 – Fornecedores externos com acesso privilegiado / ataques a terceiros de Plataformas externas integradas ao TJBA por Ausência de revisão técnica unificada de segurança em contratações SaaS

Tipo de Risco: Estratégico

O Tribunal utiliza diversas plataformas SaaS e serviços externos integrados à sua infraestrutura e sistemas. Sem uma revisão técnica unificada de segurança nessas contratações, há risco de que fornecedores com acesso privilegiado ou vulnerabilidades em terceiros sejam explorados, ocasionando exposição de dados estratégicos ou restritos e impactos à imagem do Tribunal.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Criar um processo formal de revisão de segurança para todos os serviços em nuvem e contratações SaaS, com checklist padronizado.
2. Estabelecer indicador de "% de serviços SaaS revisados pela ASI" e reportá-lo à governança de TIC.
3. Exigir, nos contratos, requisitos mínimos de segurança para terceiros (ex.: criptografia, gestão de vulnerabilidades, logs, conformidade com LGPD).

Como cada ação reduz o risco

1. O processo formal de revisão de segurança reduz a probabilidade de contratação de serviços SaaS com controles inadequados, antecipando riscos antes da entrada em produção.
2. O indicador de % de SaaS revisados pela ASI permite ao nível executivo enxergar se novas integrações e contratos estão passando efetivamente pelo crivo de segurança, funcionando como um "sinal de alerta" de exposição crescente.
3. A inclusão de requisitos mínimos de segurança em contrato reforça a responsabilidade do fornecedor e viabiliza auditorias, sanções e correções, reduzindo o impacto de incidentes gerados por terceiros..

Responsável: ASI

Situação: Planejado

KRI: % de serviços SaaS revisados tecnicamente (Mensal).

Interpretação do KRI: Este KRI indica, em termos percentuais, quantos dos serviços SaaS utilizados pelo Tribunal passaram por revisão técnica de segurança conduzida ou validada pela ASI. Quanto menor o valor, maior a chance de existirem integrações críticas operando sem análise de segurança, o que aumenta o risco de vazamento ou uso indevido de dados por terceiros. O aumento progressivo desse indicador, até níveis próximos de

100%, demonstra que o plano de tratamento está ampliando o controle e a governança sobre o ecossistema de fornecedores.

Fórmula: Percentual de serviços SaaS revisados tecnicamente = (Número de serviços SaaS revisados tecnicamente pela ASI / Número total de serviços SaaS em uso) × 100

Meta: 1 (interpretação: 100% dos serviços SaaS revisados)

5.1.3 Risco: R23 – ID: ASI-03 – Vieses algorítmicos e decisões automatizadas indevidas de Modelos de IA utilizados em análise judicial por Ausência de critérios técnicos de auditoria, governança e explicabilidade

Tipo de Risco: Estratégico

O Tribunal utiliza ou pretende utilizar modelos de IA em apoio à atividade judicial. Sem critérios claros de auditoria, governança, explicabilidade e registro, há risco de decisões automatizadas indevidas, vieses algorítmicos e questionamentos sobre a legitimidade das decisões, com impacto na confiança de magistrados, servidores e jurisdicionados.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Criar um módulo específico de IA segura dentro da plataforma de conscientização em Segurança da Informação.
2. Estabelecer governança mínima para modelos de IA (auditoria, logs, controle de acesso a datasets, versionamento, cadastro).
3. Restringir usos não autorizados de IA, exigindo aprovação e cadastro prévio de modelos.

Como cada ação reduz o risco

1. O módulo de IA segura aumenta a consciência de magistrados e equipes técnicas sobre riscos de vieses, uso indevido e necessidade de explicabilidade, reduzindo o risco de implantação de soluções críticas sem análise.
2. A governança mínima de modelos (auditoria, logs, acesso a dados) permite reconstruir decisões algorítmicas, identificar padrões de vieses e corrigir modelos quando necessário, reduzindo o impacto de decisões indevidas.
3. A restrição de usos não autorizados impede que modelos experimentais ou não avaliados sejam usados em contextos sensíveis, reduzindo a probabilidade de incidentes reputacionais e jurídicos.

Responsável: ASI

Situação: Planejado

KRI: % de modelos de IA auditados e explicáveis (Trimestral).

Interpretação do KRI: Este KRI mede a proporção de modelos de IA em uso que já passaram por um processo mínimo de auditoria, documentação e explicabilidade. Quando este percentual é baixo, a exposição a vieses não detectados e decisões automatizadas pouco transparentes é alta. À medida que o indicador cresce, evidencia-se que os modelos críticos estão sendo

administrados sob um regime de governança, reduzindo o risco de questionamentos institucionais e regulatórios.

Fórmula: Percentual de modelos de IA auditados e explicáveis = (Número de modelos de IA auditados e com explicabilidade documentada / Número total de modelos de IA em uso) × 100

Meta: ≥ 90%

5.1.4 Risco: R24 – ID: ASI-04 – Ataque cibernético disruptivo / ransomware de Serviços essenciais de TIC do TJBA por Ausência de plano integrado de continuidade (PDTIC/ENSEC-PJ)

Tipo de Risco: Estratégico

Risco de um ataque cibernético disruptivo (como ransomware) atingir múltiplos serviços essenciais de TIC sem que exista um plano integrado e testado de continuidade e recuperação, alinhado ao PDTIC e ENSEC-PJ. A consequência é a paralisação de sistemas críticos, com impacto direto na prestação jurisdicional e na imagem institucional.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Integrar COTEC e ASI em um plano único de continuidade de TIC, com papéis e responsabilidades claros.
2. Oficializar e realizar testes de mesa e simulações periódicas de cenários de ataque disruptivo/ransomware.
3. Estabelecer uma matriz de criticidade de serviços, priorizando RTO/RPO e estratégias de recuperação.

Como cada ação reduz o risco

1. A integração COTEC + ASI no plano único garante coordenação entre infraestrutura, operações e segurança durante um incidente, reduzindo o tempo de resposta e de recuperação.
2. Os testes de mesa e simulações permitem identificar antecipadamente falhas de procedimento, lacunas de comunicação ou dependências críticas não mapeadas, reduzindo a probabilidade de falhas de resposta em um ataque real.
3. A matriz de criticidade de serviços orienta investimentos (backup, replicação, nuvem, redundância) e ajuda a alinhar prioridades com a alta administração, reduzindo o impacto da paralisação.

Responsável: ASI

Situação: Planejado

KRI: Índice de maturidade do plano de continuidade (Mensal).

Interpretação do KRI: O KRI sintetiza o grau de implementação dos itens previstos no plano de continuidade (políticas, procedimentos, testes, infraestrutura, documentação). Quanto maior o índice, mais robusta é a capacidade do Tribunal de suportar ataques disruptivos sem paralisação prolongada. A evolução desse índice, alinhada aos testes realizados, mostra

se o plano vai deixando de ser apenas "documental" para se tornar efetivo na prática.

Fórmula: Índice de maturidade do plano de continuidade = (Número de itens do plano de continuidade efetivamente implementados / Número total de itens previstos no plano) × 100

Meta: ≥ 85%

5.1.5 Risco: R25 – ID: ASI-05 – Phishing / credential stuffing de Credenciais e contas institucionais por Cobertura incompleta de MFA / governança parcial de identidades

Tipo de Risco: Tático

As credenciais institucionais de magistrados, servidores e terceiros estão expostas a ataques de phishing e tentativas de credential stuffing, especialmente onde não há múltiplos fatores de autenticação (MFA) ou governança adequada de identidades (IGA). A invasão de sistemas internos pode levar a vazamentos, fraudes e interrupções de serviços.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Institucionalizar o IGA (conforme PD.22 do PDTIC), com processos formais de provisão, revisão e desprovisão de contas.
2. Completar a implantação de MFA para contas e sistemas prioritários, especialmente os mais críticos.
3. Revisar o ciclo de vida das contas (criação, alteração, desligamento, revisão periódica) para garantir que não existam acessos indevidos ou obsoletos.

Como cada ação reduz o risco

1. O IGA institucionalizado reduz contas órfãs, excessos de privilégio e acessos incompatíveis com o perfil do usuário, diminuindo a probabilidade de uso indevido de credenciais.
2. A cobertura ampla de MFA reduz drasticamente a eficácia de ataques de phishing e credential stuffing, mesmo quando a senha é comprometida, reduzindo a probabilidade de invasão de sistemas.
3. A revisão do ciclo de vida das contas garante que acessos de ex-servidores ou mudanças de função sejam refletidos nos sistemas, reduzindo superfícies de ataque e exposição prolongada.

Responsável: ASI

Situação: Planejado

KRI: % de contas com MFA ativo (Mensal).

Interpretação do KRI: O KRI mede quantas contas ativas já estão protegidas por MFA. Valores baixos indicam que a maior parte dos usuários ainda depende apenas de senha, o que os deixa vulneráveis a ataques de phishing e brute force. À medida que o percentual cresce, observa-se uma redução estrutural da probabilidade de invasão via credenciais roubadas, evidenciando o sucesso das ações de tratamento.

Fórmula: Percentual de contas com MFA ativo =(Número de contas institucionais com MFA habilitado / Número total de contas institucionais ativas) × 100

Meta: 1 (interpretação: 100% das contas com MFA ativo, ou meta progressiva definida em política)

5.1.6 Risco: R26 – ID: ASI-06 – Movimentação lateral, ataque persistente avançado de Registro e auditoria de eventos por Baixa visibilidade dos eventos críticos

Tipo de Risco: Tático

O ambiente de TIC do Tribunal gera grande volume de eventos de segurança. Com baixa visibilidade sobre eventos críticos (logs dispersos, ausência de correlação ou monitoramento centralizado), há risco de ataques avançados (movimentação lateral, APT) não serem detectados em tempo, resultando em perdas financeiras, vazamentos e indisponibilidade prolongada.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Finalizar a implantação do SOC (Security Operations Center) com capacidade de monitoramento centralizado.
2. Integrar ao SOC os principais endpoints, ambientes em nuvem e aplicações críticas, consolidando logs e alertas.
3. Criar dashboards executivos para a ASI, com visão de eventos críticos, incidentes e tendências.

Como cada ação reduz o risco

1. O SOC implantado com escopo adequado aumenta a capacidade de detectar rapidamente comportamentos anômalos e ataques persistentes, reduzindo o tempo de detecção.
2. A integração de múltiplas fontes (endpoints, nuvem, aplicações) melhora a correlação de eventos, permitindo identificar movimentações laterais que não seriam percebidas por monitoramentos isolados.
3. Os dashboards executivos dão visibilidade à gestão sobre o nível de exposição e a eficácia do monitoramento, facilitando priorização de ações corretivas e investimentos adicionais quando necessário.

Responsável: ASI

Situação: Planejado

KRI: % de eventos críticos monitorados pelo SOC (Mensal).

Interpretação do KRI: Este KRI mede a cobertura do SOC em relação aos eventos considerados críticos (por exemplo, tentativas de acesso privilegiado, falhas de autenticação em massa, alterações em configurações sensíveis). Se apenas uma pequena parte estiver sendo monitorada, a chance de ataques avançados passarem despercebidos é alta. O aumento do percentual indica que o ambiente está ficando mais “visível” para a ASI, reduzindo a probabilidade de detecção tardia.

Fórmula: Percentual de eventos críticos monitorados pelo SOC =(Número de eventos críticos efetivamente monitorados e correlacionados pelo SOC / Número total de eventos críticos definidos na matriz de monitoramento) × 100

Meta: ≥ 95%

5.1.7 Risco: R27 – ID: ASI-07 – Erros, falhas, manipulação indevida de Serviços, dados, arquivos e sistemas afetados por mudanças por Mudanças sem avaliação formal de segurança

Tipo de Risco: Tático

Mudanças em sistemas, serviços e infraestruturas podem introduzir vulnerabilidades, inconsistências ou indisponibilidades quando não passam por avaliação formal de segurança. Sem a participação sistemática da ASI no processo de mudança, há risco de implantar alterações que fragilizam o ambiente, gerando falhas, retrabalho e perda de integridade de dados.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Tornar obrigatória a avaliação de Segurança da Informação em todas as mudanças relevantes (relacionadas a PD.14, PD.31, PD.46 do PDTIC).
2. Registrar o aceite formal da ASI nas RFCs (Requisições de Mudança) como etapa do fluxo de gestão de mudanças.

Como cada ação reduz o risco

1. A obrigatoriedade da avaliação de SI em mudanças garante que potenciais impactos em segurança sejam analisados antes da implementação, reduzindo a probabilidade de introdução de novas vulnerabilidades.
2. O registro de aceite da ASI nas RFCs cria trilha de responsabilização e permite rastrear se uma mudança problemática passou ou não pela avaliação de segurança, facilitando correções e aprendizado organizacional.

Responsável: ASI

Situação: Planejado

KRI: % de mudanças com avaliação formal de segurança (Mensal).

Interpretação do KRI: O KRI mede a aderência do processo de mudança ao requisito de avaliação de SI. Se poucas mudanças são avaliadas, o Tribunal permanece exposto a falhas introduzidas por alterações não revisadas. Quando o índice se aproxima da meta, a probabilidade de incidentes decorrentes de mudanças sem revisão cai significativamente, indicando que o plano de tratamento está efetivo.

Fórmula: Percentual de mudanças com avaliação formal de segurança = (Número de mudanças avaliadas formalmente pela ASI / Número total de mudanças realizadas no período) × 100

Meta: ≥ 98%

5.1.8 Risco: R28 – ID: ASI-08 – Phishing, erros, esquecimentos e engenharia social de Usuários e colaboradores por Baixa adesão de servidores, usuários e terceiros (atual 40% → meta 99%)

Tipo de Risco: Tático

Usuários e colaboradores com baixa conscientização em Segurança da Informação estão mais suscetíveis a esquemas de phishing, engenharia social, erros e esquecimentos que podem levar a vazamento de dados, comprometimento de contas e incidentes de segurança. Apesar de já existir programa de conscientização, a adesão atual (cerca de 40%) é insuficiente para o nível de exposição.

Tipo de Tratamento: Controles Detectivos e Corretivos

Plano de Tratamento

1. Tornar o treinamento de Segurança da Informação obrigatório para perfis definidos (servidores, magistrados, terceirizados).
2. Solicitar convocação institucional formal das áreas, reforçando a obrigatoriedade e prazos.
3. Criar trilhas de conscientização por papel (usuário comum, gestor, técnico, alta administração).
4. Incluir um módulo específico sobre IA segura, ampliando a compreensão dos riscos de uso indevido de IA.

Como cada ação reduz o risco

1. A obrigatoriedade do treinamento, aliada à convocação institucional, aumenta a cobertura de usuários sensibilizados, reduzindo a probabilidade de sucesso de campanhas de phishing e de engenharia social.
2. As trilhas por papel tornam o conteúdo mais aderente ao dia a dia de cada público, aumentando a efetividade do aprendizado e da mudança de comportamento.
3. O módulo de IA segura contribui para reduzir riscos emergentes relacionados ao uso indiscriminado de ferramentas de IA em contexto institucional.

Responsável: ASI

Situação: Planejado

KRI: % de usuários com treinamento obrigatório concluído (Mensal)

Interpretação do KRI: Este KRI mostra a cobertura do programa de conscientização entre os públicos obrigatórios. Valores baixos indicam alta exposição a ataques de phishing e erros por desconhecimento. A aproximação da meta (99%) indica que o Tribunal está criando uma "barreira humana" mais robusta, reduzindo a probabilidade de incidentes causados por comportamento inseguro.

Fórmula: Percentual de usuários com treinamento obrigatório concluído = (Número de usuários que concluíram o treinamento obrigatório de SI / Número total de usuários que deveriam realizar o treinamento) × 100

Meta: ≥ 99%

5.1.9 Risco: R29 – ID: ASI-09 – Ataques de configuração incorreta (misconfiguration) de Instâncias e serviços configurados por Ausência de CSPM / validação técnica contínua

Tipo de Risco: Operacional

Em ambientes de nuvem (Azure, AWS, outros), configurações incorretas de recursos (storage públicos, portas expostas, permissões excessivas) são um vetor comum de ataque. Sem uma ferramenta de Cloud Security Posture Management (CSPM) e validação contínua, há risco de exposição de dados e sistemas por misconfiguration.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Implantar uma solução de CSPM para avaliar continuamente a postura de segurança em nuvem.
2. Criar checklist formal de configuração segura para recursos cloud, baseado em boas práticas (CIS, recomendações do provedor).
3. Integrar o monitoramento do CSPM ao SOC, gerando alertas para configurações críticas.

Como cada ação reduz o risco

1. O CSPM identifica automaticamente configurações inseguras, reduzindo o tempo em que um erro de configuração fica exposto.
2. O checklist formal de configuração segura padroniza boas práticas e reduz a probabilidade de misconfiguration no momento da criação de recursos.
3. A integração com o SOC garante que alertas de configuração crítica sejam acompanhados e tratados, evitando que permaneçam em aberto por longos períodos.

Responsável: ASI

Situação: Planejado

KRI: % de recursos cloud validados por CSPM (Mensal)

Interpretação do KRI: O KRI mede quantos recursos de nuvem estão sob validação ativa do CSPM. Recursos fora do escopo da ferramenta podem estar configurados de forma insegura sem qualquer alerta. À medida que o percentual aumenta, a cobertura da validação automática melhora, reduzindo a probabilidade de exposição por misconfiguration.

Fórmula: Percentual de recursos cloud validados por CSPM = (Número de recursos de nuvem validados pelo CSPM / Número total de recursos de nuvem em uso) × 100

Meta: ≥ 95%

5.1.10 Risco: R30 – ID: ASI-10 – Usuários mal-intencionados, erros, falhas, imperícia de ações de terceiros de Bases, arquivos, sistemas, equipamentos, serviços e repositórios de dados por Falta de visibilidade de movimentações internas, falta de integração dos controles de segurança dos ambientes

Tipo de Risco: Operacional

Mesmo quando as ameaças externas são controladas, ações internas – intencionais ou acidentais – podem gerar vazamentos, exclusões indevidas, criptografia de dados e indisponibilidade de ambientes. Sem visibilidade adequada sobre movimentações internas e sem integração dos controles, o Tribunal fica vulnerável a incidentes internos significativos.

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Implantar uma solução de DLP institucional, cobrindo canais críticos (rede, e-mail, endpoints).
2. Monitorar fluxos de dados sensíveis, definindo regras específicas para bases, repositórios e serviços críticos.
3. Criar alertas de comportamento anômalo (ex.: grandes volumes de cópias, acessos fora de horário, download massivo)

Como cada ação reduz o risco

1. O DLP institucional detecta tentativas de exfiltração de dados e movimentações suspeitas, reduzindo a probabilidade de vazamentos internos passarem despercebidos.
2. O monitoramento de fluxos sensíveis torna mais difícil que dados críticos sejam copiados ou enviados sem registro, reduzindo a superfície de ataque interno.
3. Os alertas de comportamento anômalo permitem reagir rapidamente a ações suspeitas, reduzindo o impacto de incidentes internos antes que se tornem crises.

Responsável: ASI

Situação: Planejado

KRI: N° de alertas de movimentação interna anômala (Mensal).

Interpretação do KRI: Este KRI mede a quantidade de alertas críticos gerados por movimentações internas consideradas anômalas. Um número muito alto pode indicar tanto aumento do risco (mais comportamentos suspeitos) quanto ajustes necessários nas regras. O objetivo, após estabilização das regras, é que o número de alertas críticos se mantenha baixo e, preferencialmente, em tendência de queda, indicando que o comportamento dos usuários está mais alinhado à política de segurança.

Fórmula: Número de alertas de movimentação interna anômala = Contagem de alertas críticos de movimentações internas consideradas anômalas no período

Meta: ≤ 5 alertas críticos por mês

5.1.11 Risco: R31 – ID: ASI-11 – Ataques de acesso indevido de Rede e serviços internos por VPN sem camadas adicionais

Tipo de Risco: Estratégico

O acesso remoto ao ambiente interno via VPN é indispensável, mas, quando não protegido por camadas adicionais (ZTNA, MFA, políticas de contexto), pode se tornar um ponto de entrada para invasores. Caso credenciais sejam comprometidas, a VPN sem camadas extras facilita o acesso direto à rede interna.

Tipo de Tratamento: Controles Aceitação e Monitoria

Plano de Tratamento

1. Finalizar a implantação de ZTNA, adicionando camadas de controle ao acesso remoto.
2. Revisar as regras de acesso remoto, limitando privilégios e segmentando a rede.
3. Auditar regularmente as conexões remotas, verificando acessos incomuns ou incompatíveis.

Como cada ação reduz o risco

1. A ZTNA adiciona checagens de contexto (dispositivo, localização, identidade) além da VPN, aumentando a segurança e reduzindo a probabilidade de acesso indevido.
2. A revisão de regras reduz o escopo de acesso concedido via VPN, diminuindo o impacto caso uma credencial seja comprometida.
3. As auditorias de conexões remotas permitem identificar usos inadequados ou suspeitos, disparando ações corretivas.

Responsável: ASI

Situação: Em Execução

KRI: % de conexões remotas protegidas por ZTNA/MFA (Mensal).

Interpretação do KRI: O KRI mostra a parcela de conexões remotas que já estão protegidas por controles adicionais além da VPN. Quanto maior o percentual, menor a probabilidade de que uma credencial comprometida resulte em acesso irrestrito. A evolução do indicador em direção a 100% demonstra o amadurecimento da arquitetura de acesso remoto seguro.

Fórmula: Percentual de conexões remotas protegidas por ZTNA/MFA = (Número de conexões remotas que utilizam ZTNA e/ou MFA / Número total de conexões remotas realizadas) × 100

Meta: 1 (interpretação: 100% das conexões remotas protegidas por ZTNA/MFA)

5.1.12 Risco: R32 – ID: ASI-12 – Perda, roubo, sincronização não controlada de Dados institucionais acessados por dispositivos pessoais por Ausência de MDM / regras formais

Tipo de Risco: Operacional

Dispositivos pessoais (BYOD) ou em comodato, sem gestão formal (MDM) e sem regras claras de uso, podem conter dados institucionais sincronizados. Em caso de perda, roubo ou mau uso, há risco de exposição de dados, indisponibilidade de informações e dificuldade de reação (ex.: limpeza remota)..

Tipo de Tratamento: Controles Detectivos e Compensatórios

Plano de Tratamento

1. Criar política formal de BYOD, definindo limites, responsabilidades e tipos de dispositivos permitidos.
2. Definir quais dispositivos podem acessar dados institucionais e em quais condições (ex.: criptografia, bloqueio de tela, senha).
3. Implantar MDM para dispositivos BYOD e institucionais em mobilidade, permitindo controle e limpeza remota.

Como cada ação reduz o risco

1. A política de BYOD estabelece balizas claras para uso de dispositivos pessoais, reduzindo comportamentos de risco e facilitando a responsabilização.
2. A definição de dispositivos permitidos e requisitos mínimos (ex.: criptografia, bloqueio) reduz a probabilidade de dados sensíveis serem mantidos em equipamentos frágeis.
3. O MDM permite revogar acessos, aplicar configurações mínimas de segurança e executar limpeza remota em caso de perda ou roubo, reduzindo o impacto de incidentes.

Responsável: ASI

Situação: Em Execução

KRI: % de dispositivos BYOD com MDM ativo (Mensal).

Interpretação do KRI: Este KRI mede quantos dos dispositivos pessoais que acessam dados institucionais estão sob controle do MDM. Dispositivos fora do MDM representam pontos cegos de segurança, com maior probabilidade de perda ou roubo de dados sem reação adequada. O aumento do percentual indica que o Tribunal está ampliando a governança sobre o parque de dispositivos móveis, reduzindo a exposição a vazamentos.

Fórmula: Percentual de dispositivos BYOD com MDM ativo = (Número de dispositivos BYOD com MDM instalado e ativo / Número total de dispositivos BYOD autorizados a acessar dados institucionais) × 100

Meta: ≥ 95%