PLANO DE RISCOS PRIORIZADO (RISCO INERENTE)

PROCESSO STJ: 020391/2025 - OBJETO/ ESCOPO: Prestação do serviço de acesso à plataforma de livros digitais Minha Biblioteca das áreas Jurídica e Ciências Sociais Aplicadas.

Aplicação	Nivel de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle
Aquisição Contratação	(-15) Ameaça Média	R03	Descontinuidade da prestação do serviço	Ausência de planejamento para encerramento e transição contratual, inexecução total ou parcial do contrato, falência ou concordata da empresa	Prejuízos ao erário, produtos ou serviços indisponíveis, assunção das atividades por parte do Tribunal, contratação emergencial	Não acompanhado	Preventivo	Elaborar plano de encerramento ou transição contratual	SEDAC	(vazio)	(vazio)	Não iniciado
Processo Trabalho	(-15) Ameaça Média	R11	Remoção não autorizada / Roubo de dados pessoais	Retirada ou cópia de dados pessoais sem autorização / Dados	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem	Não acompanhado	Preventivo	Capacitar usuários sobre segurança da informação	(vazio)	(vazio)	(vazio)	Não iniciado
								Realizar Backup				Não iniciado
	(-9) Ameaça Média	R06	Compartilhamento indevido de dados pessoais	Compartilhamento sem amparo legal ou consentimento do titular dos dados pessoais				Revisar hipóteses de compartilhamento de dados pessoais	SEDAC			Não iniciado
		R10	Perda da confidencialidade de dados pessoais	Acesso não autorizado (permissões indevidas) a um				Realizar controle de acesso físico	(vazio)			Não iniciado
								Capacitar usuários sobre segurança da informação				Não iniciado
Aquisição Contratação	(-3) Ameaça Baixa	R01	Contratação que não atenda à necessidade do Tribunal	Estudos técnicos preliminares com informações insuficientes sobre a demanda	Desperdício de recursos públicos	Em acompanhamento	Preventivo	Elaborar estudos preliminares com justificativas adequadas e identificação das necessidades junto aos demandantes	SEDAC	15/05/2025	(vazio)	Em andamento
		R05	Fornecimento de produtos ou execução de serviços com baixa qualidade ou fora da especificação	Ausência ou ineficiência de requisitos para fornecimento de produtos ou execução de serviços	Comprometimento na qualidade do serviço, dano ao erário	Não acompanhado	Contingente	Recusa de produtos e serviços entregues fora do especificado em contrato		(vazio)		Não iniciado
							Preventivo	Definir procedimentos para teste, aceite e recusa de produtos ou serviços				Não iniciado
Processo Trabalho	(-3) Ameaça Baixa	R12	Retenção prolongada de dados pessoais sem necessidade	Inexistência de procedimento de descarte após o prazo de retenção necessária dos dados pessoais	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem	Não acompanhado	Preventivo	Definir procedimento de descarte das informações desnecessárias	(vazio)	(vazio)	(vazio)	Não iniciado

Aplicação	Nivel de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle
Aquisição Contratação	(-1) Ameaça Baixa	R02	Desconsideração de riscos e controles da contratação	Desatualização do tratamento dos riscos da contratação	Concretização de riscos com impacto na contratação e/ou serviços prestados	Em acompanhamento	Preventivo	Gerenciar riscos referentes ao negócio e à contratação durante todas as fases, de acordo com a metodologia de riscos do Tribunal	SEDAC	05/06/2025	(vazio)	Em andamento
Processo Trabalho	(-1) Ameaça Baixa	R04	Desconsideração de riscos e controles do processo de trabalho	Desatualização do planejamento de riscos do processo de trabalho	Concretização de riscos com impacto nos objetivos do processo de trabalho	Não acompanhado	Preventivo	Gerenciar riscos referentes ao processo de trabalho durante todas as fases, de acordo com a metodologia de riscos do Tribunal	SEDAC	(vazio)	(vazio)	Não iniciado
		R08	Falha ou erro de processamento de dados pessoais	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem			Realizar Backup				Não iniciado
		R09	Modificação não autorizada de dados pessoais	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada.	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem			Capacitar usuários sobre segurança da informação	(vazio)			Não iniciado
Projeto Programa	(-1) Ameaça Baixa	R07	Coleção excessiva de dados pessoais	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem	Não acompanhado	Preventivo	Limitar a coleta ao estritamente necessário para o atendimento da finalidade	SEDAC	(vazio)	(vazio)	Não iniciado

MONITORAMENTO DOS RISCOS INERENTE X RESIDUAL

PROCESSO STJ: 020391/2025 - OBJETO/ ESCOPO: Prestação do serviço de acesso à plataforma de livros digitais Minha Biblioteca das áreas Jurídica e Ciências Sociais Aplicadas.

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nivel de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco
		R01	Contratação que não atenda à necessidade do Tribunal	Estudos técnicos preliminares com informações insuficientes sobre a demanda	Desperdício de recursos públicos	(-3) Ameaça Baixa		Forte (Controles implementados podem ser considerados a "melhor prática", que tratam todos os aspectos relevantes do risco)	Muito Baixo	(-0,6) Ameaça Baixa	Em acompanhamento
		R02	Desconsideração de riscos e controles da contratação	Desatualização do tratamento dos riscos da contratação	Concretização de riscos com impacto na contratação e/ou serviços prestados	(-1) Ameaça Baixa				(-0,2) Ameaça Baixa	Em acompanhamento
		R03	Descontinuidade da prestação do serviço	Ausência de planejamento para encerramento e transição contratual, inexecução total ou parcial do contrato, falência ou concordata da empresa	Prejuízos ao erário, produtos ou serviços indisponíveis, assunção das atividades por parte do Tribunal, contratação emergencial	(-15) Ameaça Média		Inexistente (Controles inexistentes, não implementados ou mal desenhados)	Muito Alto	(-15) Ameaça Média	Não acompanhado
		R04	Desconsideração de riscos e controles do processo de trabalho	Desatualização do planejamento de riscos do processo de trabalho	Concretização de riscos com impacto nos objetivos do processo de trabalho	(-1) Ameaça Baixa		Satisfatório (Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, tratam satisfatoriamente o risco)	Baixo	(-0,4) Ameaça Baixa	Não acompanhado

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nivel de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco
15/07/2025	Rodrigo Vasconcelos Rodrigues Pinheiro	R05	Fornecimento de produtos ou execução de serviços com baixa qualidade ou fora da especificação	Ausência ou ineficiência de requisitos para fornecimento de produtos ou execução de serviços	Comprometimento na qualidade do serviço, dano ao erário	(-3) Ameaça Baixa	Elaboração de nova versão do Plano de Riscos	Mediano (Controles implementados que mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas)	Médio	(-1,8) Ameaça Baixa	Não acompanhado
		R06	Compartilhamento indevido de dados pessoais	Compartilhamento sem amparo legal ou consentimento do titular dos dados pessoais	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem	(-9) Ameaça Média		Satisfatório (Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, tratam satisfatoriamente o risco)	Baixo	(-3,6) Ameaça Baixa	Não acompanhado
		R07	Coleção excessiva de dados pessoais	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.		(-1) Ameaça Baixa		Forte (Controles implementados podem ser considerados a "melhor prática", que tratam todos os aspectos relevantes do risco)	Muito Baixo	(-0,2) Ameaça Baixa	Não acompanhado
		R08	Falha ou erro de processamento de dados pessoais	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem			Satisfatório (Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de	Baixo	(-0,4) Ameaça	Não acompanhado

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nivel de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco
		R09	Modificação não autorizada de dados pessoais	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada.	Desconformidade com a LGPD; sujeição a punições aplicáveis; dano à imagem			e, embora passíveis de aperfeiçoamento, tratam satisfatoriamente o risco)	Baixo	Baixa	Não acompanhado
		R10	Perda da confidencialidade de dados pessoais	Acesso não autorizado (permissões indevidas) a um ambiente físico ou lógico		(-9) Ameaça Média		Mediano (Controles implementados que mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas)	Médio	(-5,4) Ameaça Média	Não acompanhado
		R11	Remoção não autorizada / Roubo de dados pessoais	Retirada ou cópia de dados pessoais sem autorização / Dados roubados nas dependências interna do controlador/operador, falhas nos controles de segurança dos sistemas, entre outras.		(-15) Ameaça Média				(-9) Ameaça Média	Não acompanhado
		R12	Retenção prolongada de dados pessoais sem necessidade	Inexistência de procedimento de descarte após o prazo de retenção necessária dos dados pessoais		(-3) Ameaça Baixa		Forte (Controles implementados podem ser considerados a "melhor prática", que tratam todos os aspectos relevantes do risco)	Muito Baixo	(-0,6) Ameaça Baixa	Não acompanhado