

PROCESSO STJ: 005492/2024 - OBJETO/ ESCOPO: Solução capaz de capturar o tráfego de rede de um seguimento específico, realizar tratamento prévio desse tráfego como remoção de duplicações, anonimização de informações, remoção de dados irrelevantes para análise de segurança e, por fim, encaminhar o tráfego resultante para análise por tecnologias de inteligência artificial, comportamental entre outras técnicas promovendo a identificação e, eventualmente, o bloqueio de tais ameaças em nível de rede													
Aplicação	Nível de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle	
	(-15) Ameaça Média	R06	Conflito de interesse na gestão e fiscalização de contratos de prestação de serviços	Indicação de profissionais com vínculo afetivo para trabalharem em empresas contratadas, falta de fiscalização, sensação de impunidade, favorecimento de terceiros	Elevação de custos, ilegalidade, desrespeito ao interesse público, não selecionar melhor prestador de serviço, danos à imagem do tribunal	Em acompanhamento	Preventivo	Incluir no termo de referência as formas de comunicação entre contratante e contratada a ser realizada ao longo da execução contratual	EPC e EFC	Início dos estudos preliminares	Término da execução contratual	Em andamento	
		R03	Indisponibilidade orçamentária integral ou parcial para cumprimento dos objetivos da aquisição/ contratação	Contingenciamento ou limitação orçamentária, aumento dos custos da contratação	Redução do escopo da aquisição ou impossibilidade de contratação	Não concretizado		Gerenciar riscos referentes ao negócio e à contratação durante todas as fases, de acordo com a metodologia de riscos do Tribunal			Assinatura do instrumento contratual decorrente do resultado do certame licitatório	Concluído	
	(-9) Ameaça Média	R05	Contratada não manter as condições de habilitação e qualificação exigida na licitação durante o contrato	Ausência de consequências para a contratada caso não mantenha as condições de habilitação e qualificação exigidas na licitação	Retorno de todos os impactos tratados com a exigência da qualificação e habilitação	Em acompanhamento		Elaborar memória de cálculo das estimativas de preço com todos os itens a serem contratados	EPC			Publicação do instrumento convocatório	Concluído
								Definir modelo de pagamento durante a fase de execução contratual coerente com o modelo de comercialização da solução de TIC de forma a não onerar propostas comerciais ofertadas pelas licitantes.				Concluído	
								Avaliar o uso e impacto de valores praticados pela Administração Pública em outras contratações quanto ao nível de similitude em relação à contratação pretendida com vistas a estabelecer estimativas adequadas (sem distorção em relação praticado pelo Merrcado).				Assinatura do instrumento contratual decorrente do resultado do certame licitatório	Concluído

Aplicação	Nível de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle
		R07	Licitação deserta	Levantamento de mercado deficiente, exigências descabidas ou requisitos fora do padrão de mercado	Atraso na contratação, republicação de edital e revisão de documentos		Contingente	Solicitar realocação de recursos entre outras demandas da Administração	STI, SOF, DG	Assinatura do instrumento contratual decorrente do resultado do certame licitatório	Término da execução contratual	Não iniciado
								Repactuação de valores de forma a manter o equilíbrio econômico-financeiro da contratação		Assinatura do contrato	Liquidação e pagamento de valores devidos à contratada	Não iniciado
							Preventivo	Realizar previsão orçamentária para pagamento contratual		Início dos estudos preliminares	Assinatura do instrumento contratual decorrente do resultado do certame licitatório	Em andamento
		R09	Descumprimento dos prazos contratuais	Definição de prazos incompatíveis com a demanda ou contratada não cumprir prazos acordados	Comprometimento da qualidade do atendimento	Não acompanhado	(vazio)	(vazio)	(vazio)	(vazio)	(vazio)	(vazio)
			R01	Contratação que não atenda à necessidade do Tribunal	Estudos técnicos preliminares com informações insuficientes sobre a demanda	Desperdício de recursos públicos	Não concretizado	Preventivo	Elaborar estudos preliminares com justificativas adequadas e identificação das necessidades junto aos demandantes	EPC	Início dos estudos preliminares	Publicação do instrumento convocatório
	Identificar e definir requisitos para fornecimento de produtos								Concluído			
	Identificar e definir requisitos para prestação do serviço								Concluído			
	R04		Contratação de empresa incapaz de fornecer produto ou executar serviço	Empresas sem qualificação técnica adequada para a prestação de serviços	Não obtenção do objeto contratado e descumprimento de obrigações contratuais	Em acompanhamento	Contingente	Aplicar sanções e penalidades à contratada caso não cumpra os prazos definidos	EFC	Início da execução contratual	Término da execução contratual	Não iniciado
								Acompanhar o cronograma de execução para identificar potenciais origens do atraso	EPC e EFC			Não iniciado

Aplicação	Nível de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle	
	(-3) Ameaça Baixa			administrativo de contratação	ambiente atual		Preventivo	EFC solicita exclusão dos dados pessoais ao término da vigência contratual		30 dias para o término da vigência contratual	Término da execução contratual	Não iniciado	
		R16	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	Não acompanhado	Contingente	Solicitar aplicação de sanções à empresa contratada	EFC	Início da execução contratual		Não iniciado	
		R17	Perda da confidencialidade de dados pessoais	Acesso não autorizado (permissões indevidas) a um ambiente físico ou lógico						Término da execução contratual		Não iniciado	
		R18	Retenção prolongada de dados pessoais sem necessidade	Inexistência de procedimento de descarte após o prazo de retenção necessária dos dados pessoais						30 dias para o término da vigência contratual		Não iniciado	
		R19	Vazamento de dados do STJ	Ações que gerem a exposição de dados sensíveis ou não relacionados as operações do STJ	Dano de imagem, desconformidade com a LGPD; sujeição a punições aplicáveis		Preventivo	EFC solicita exclusão dos dados pessoais ao término da vigência contratual		Assinatura do contrato		Não iniciado	
							Contingente	Informação sobre perfis ou informações vazadas referentes aos domínios do STJ. Acompanhar o processo de Gerenciamento de Incidentes de Segurança				Não iniciado	
							Preventivo	Adoção de serviços de monitoramento de vazamento de dados deep e darkweb. Contrato com empresa para elaboração de relatório mensal				Não iniciado	
								Adoção de monitoramento integrado dos elementos de segurança do Tribunal. Contratação de empresa para implantar SOC				Início dos estudos preliminares	Em andamento
								Adoção de boas práticas dos usos de credenciais e acessos aos sistemas críticos do STJ. Adoção de duplo fator de autenticação				Assinatura do contrato	Não iniciado

Aplicação	Nível de Risco Inerente (NRI)	Id do Risco	Risco	Causa	Consequência	Situação Risco	Tipo Controle	Controle	Responsável Controle	Início Controle	Fim Controle	Situação Controle
	(-1) Ameaça Baixa	R11	Falhas na comunicação entre as partes e ausência de evidências das ocorrências na gestão contratual	Ausência de procedimentos formais de comunicação entre as partes contratantes	retardo e falhas na execução contratual e impossibilidade de identificar a parte descumpridora do contrato		Contingente	Analisar fundamentos da impugnação e realizar a correção	EPC, COLI	Publicação do instrumento convocatório	Assinatura do instrumento contratual decorrente do resultado do certame licitatório	Não iniciado
							Preventivo	Realizar pesquisa de potenciais fornecedores e experiências de outros órgãos públicos	EPC	Início dos estudos preliminares		Concluído
								Incluir justificativas e referências para fundamentar a inclusão de exigências não usuais e com risco de questionamento				Concluído
		R10	Fornecimento de produtos ou execução de serviços com baixa qualidade ou fora da especificação	Empresa não executar os serviços conforme requisitos acordados	Comprometimento na qualidade do serviço, dano ao erário		Contingente	Recusa de produtos e serviços entregues fora do especificado em contrato	EFC	Início da execução contratual	Término da execução contratual	Não iniciado
							Preventivo	Definir procedimentos para aceite e recusa de produtos ou serviços	EPC	Início dos estudos preliminares	Publicação do instrumento convocatório	Concluído
								Realizar conferência adequada dos produtos e serviços entregues	EFC	Início da execução contratual	Término da execução contratual	Não iniciado

PROCESSO STJ: 005492/2024 - OBJETO/ ESCOPO: Solução capaz de capturar o tráfego de rede de um seguimento específico, realizar tratamento prévio desse tráfego como remoção de duplicações, anonimização de informações, remoção de dados irrelevantes para análise de segurança e, por fim, encaminhar o tráfego resultante para análise por tecnologias de inteligência artificial, comportamental entre outras técnicas promovendo a identificação e, eventualmente, o bloqueio de tais ameaças em nível de rede

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nível 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	(-5) Ameaça Baixa	Possibilidade de oferta de outros produtos que requeiram não só especialização interna			(-3) Ameaça Baixa	Não concretizado
		R02	Estimativas inadequadas de preços	Coleta insuficiente de preços e propostas	Dificuldade em justificar as estimativas e os valores praticados	(-3) Ameaça Baixa	Identificado grande variação nos valores, ampliar pesquisa e avaliar complexidade das atividades			(-1,8) Ameaça Baixa	Não concretizado
		R03	Indisponibilidade orçamentária integral ou parcial para cumprimento dos objetivos da aquisição/ contratação	Contingenciamento ou limitação orçamentária, aumento dos custos da contratação	Redução do escopo da aquisição ou impossibilidade de contratação	(-9) Ameaça Média	Priorizar custos e aquisições passíveis ou de custos menores que o planejado para remanejamento			(-5,4) Ameaça Média	Não concretizado
		R04	Contratação de empresa incapaz de fornecer produto ou executar serviço	Empresas sem qualificação técnica adequada para a prestação de serviços	Não obtenção do objeto contratado e descumprimento de obrigações contratuais	(-5) Ameaça Baixa	Comunicar Gestor para devidas providências se			(-3) Ameaça Baixa	Em acompanhamento

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nível de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco
11/04/2024	EPC	R05	Contratada não manter as condições de habilitação e qualificação exigida na licitação durante o contrato	Ausência de consequências para a contratada caso não mantenha as condições de habilitação e qualificação exigidas na licitação	Retorno de todos os impactos tratados com a exigência da qualificação e habilitação	(-9) Ameaça Média	identificar descumprimento de cláusulas contratuais	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	Em acompanhamento
		R07	Licitação deserta	Levantamento de mercado deficiente, exigências descabidas ou requisitos fora do padrão de mercado	Atraso na contratação, republicação de edital e revisão de documentos		Estabelecer prazo razoável para abertura do certame devido ao nível de complexidade da contratação				Em acompanhamento
		R11	Falhas na comunicação entre as partes e ausência de evidências das ocorrências na gestão contratual	Ausência de procedimentos formais de comunicação entre as partes contratantes	retardo e falhas na execução contratual e impossibilidade de identificar a parte descumpridora do contrato	(-1) Ameaça Baixa	Definir outros canais de comunicação mais eficientes			(-0,6) Ameaça Baixa	Não acompanhado
		R14	Restringir a competitividade	Estabelecer requisitos excessivamente detalhados	Licitação deserta ou fracassada		Levantar os principais aspectos relevantes na contratação				Em acompanhamento

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nível de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco		
		R15	Morosidade no processo licitatório	Problemas encontrados durante tramitação do processo administrativo de contratação	Atrasos no processo de contratação e na sustentação do ambiente atual	(-3) Ameaça Baixa	Acompanhar trâmite processual			(-1,8) Ameaça Baixa	Em acompanhamento		
		R16	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						Não acompanhado		
		R17	Perda da confidencialidade de dados pessoais	Acesso não autorizado (permissões indevidas) a um ambiente físico ou lógico								Prever no TR requisitos LGPD que devm ser observados na execução contratual	Não acompanhado
		R18	Retenção prolongada de dados pessoais sem necessidade	Inexistência de procedimento de descarte após o prazo de retenção necessária dos dados pessoais									

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nível de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco
		R19	Vazamento de dados do STJ	Ações que gerem a exposição de dados sensíveis ou não relacionados as operações do STJ	Dano de imagem, desconformidade com a LGPD; sujeição a punições aplicáveis		Prever no TR requisitos de segurança da informação de detectem o vazamento de dados	Satisfatório (Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, tratam satisfatoriamente o risco)	Baixo	(-1,2) Ameaça Baixa	Não acompanhado
	(vazio)	R06	Conflito de interesse na gestão e fiscalização de contratos de prestação de serviços	Indicação de profissionais com vínculo afetivo para trabalharem em empresas contratadas, falta de fiscalização, sensação de impunidade, favorecimento de terceiros	Elevação de custos, ilegalidade, desrespeito ao interesse público, não selecionar melhor prestador de serviço, danos à imagem do tribunal	(-15) Ameaça Média	(vazio)	(vazio)	(vazio)	(vazio)	Em acompanhamento
		R08	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	(-5) Ameaça Baixa					Não acompanhado
		R09	Descumprimento dos prazos contratuais	Definição de prazos incompatíveis com a demanda ou contratada não cumprir prazos acordados	Comprometimento da qualidade do atendimento	(-9) Ameaça Média					Não acompanhado
		R10	Fornecimento de produtos ou execução de serviços com baixa qualidade ou fora da especificação	Empresa não executar os serviços conforme requisitos acordados	Comprometimento na qualidade do serviço, dano ao erário						Não acompanhado

Data Monitoramento	Equipe de Monitoramento	Id do Risco	Risco	Causa	Consequência	Nível de Risco Inerente (NRI)	Análise crítica	Nível Confiança Controles (NCC_Descrição)	Risco Controle (RC_Descrição)	Nível de Risco Residual (NRR)	Situação Risco