PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 111, DE 08 DE JUNHO DE 2022

Atualiza a Norma Complementar de Gestão de Riscos de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região (TRT7).

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de compatibilizar o processo de gestão de riscos de segurança da informação à Política de Gestão de Riscos do TRT7, estabelecida pela Resolução Normativa TRT7 nº 11, de 04 de junho de 2021;

CONSIDERANDO o Ato TRT7.GP nº 71, de 14 de junho de 2021, que institui o Plano de Gestão de Riscos do Tribunal Regional do Trabalho da 7ª Região;

CONSIDERANDO a necessidade de compatibilizar o processo de gestão de riscos de segurança da informação com a atual estrutura organizacional do TRT7;

CONSIDERANDO as diretrizes presentes da norma da Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira (NBR) ISO/IEC 27005:2011, que trata de gestão de riscos de segurança da informação;

CONSIDERANDO a Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nº 03, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal, em especial o capítulo III, que regulamenta o processo de gestão de riscos de segurança da informação;

CONSIDERANDO que o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, atribui à alta administração a tarefa de estabelecer diretrizes para o processo de gestão de riscos de segurança da informação (Art. 17, inciso V) e dá outras providências;

CONSIDERANDO a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e determina no art. 37: "Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.";

CONSIDERANDO a Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e determina no art. 10: "Para fortalecer as ações de governança cibernética, deve-se estabelecer um Sistema de Gestão em Segurança da Informação baseado em riscos, de acordo com recomendação do CNJ.",

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Atualizar a Norma Complementar de Gestão de Riscos de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região (TRT7).

CAPÍTULO II
DOS CONCEITOS E DAS DEFINIÇÕES

Art. 2º Para fins deste ato, fica estabelecido o significado dos seguintes termos e expressões:

I - Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II - Riscos de Segurança da Informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, que possam comprometer a confidencialidade, disponibilidade e a integridade das informações, com impacto negativo na imagem, nas atividades administrativas e/ou na prestação jurisdicional do TRT7;

III - Gestão de Riscos de Segurança da Informação (GRSI): conjunto de procedimentos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

IV - Gestores(as) de Riscos: são considerados gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os diretores, secretários e os coordenadores responsáveis por (ou proprietários de) ativos de informação.

CAPÍTULO III
DOS OBJETIVOS

Art. 3º Fica instituída a Gestão de Riscos de Segurança da Informação (GRSI) no âmbito do TRT7, com os seguintes objetivos:

I - dotar o tribunal de ferramenta eficaz no intuito de minimizar os riscos das principais atividades desenvolvidas pela Secretaria de Tecnologia da Informação e Comunicação (SETIC) e, assim, dar maior segurança a todos(as) que usam seus serviços (público interno e externo);

II - identificar, implementar ou melhorar as medidas de proteção necessárias para tratar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

III - evitar, reduzir, reter ou transferir os riscos de segurança da informação, de acordo com as diretrizes presentes no Plano de Gestão de Riscos do TRT7;

IV - aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas;

V - melhorar a eficiência operacional por meio do gerenciamento de riscos proativos;

VI- apoiar a gestão de continuidade de negócio do TRT7;

VII - resguardar a administração superior e os demais gestores(as) da organização quanto à tomada de decisão e à prestação de contas.

CAPÍTULO IV
DOS PRINCÍPIOS E DAS DIRETRIZES

Art. 4º O processo de GRSI deve estar alinhado à Política de Gestão de Riscos institucional, compatível com a missão e com os objetivos estratégicos do TRT7, além de considerar os seguintes princípios:

I - aplicação sistemática, contínua e integrada ao Sistema de Gestão de Segurança da Informação (SGSI) do TRT7 ;

II - os riscos de segurança da informação devem ser analisados e avaliados em função de sua relevância para os principais processos de negócio deste tribunal e devem ser tratados de forma a assegurar respostas efetivas;

III - alinhamento à Política de Segurança da Informação e Comunicação (POSIC) e à Política de Privacidade e Proteção de Dados Pessoais institucionais;

IV - conformidade legal;

V - transparência;

VI - abordagem explícita da incerteza;

VII - melhoria contínua.

Art. 5º A GRSI observará as seguintes diretrizes:

I - adotar a norma ABNT NBR 27005:2011 como referência para implementação, assegurando que a gestão de riscos de segurança da informação seja um processo contínuo que define o contexto interno e externo, além de avaliar e tratar os riscos usando um plano de tratamento a fim de implementar as decisões;

II - identificar e avaliar riscos em função das consequências ao tribunal e da probabilidade de sua ocorrência;

III - estabelecera ordem prioritária para o tratamento do risco;

IV - envolveras partes interessadas no processo decisório e mantê-las informadas sobre a situação da GRSI;

V - monitorar os riscos e as ações de tratamento de forma eficaz;

VI - treinar gestores(as) e pessoal a respeito dos riscos e das ações para mitigá-los;

VII - considerar fatores humanos e culturais;

VIII - ser dinâmico, iterativo e capaz de reagir às mudanças tempestivamente;

IX - tratar vulnerabilidades influenciará na diminuição dos riscos.

CAPÍTULO V
DO PROCESSO

Art. 6º A GRSI adotará os processos, artefatos, escalas de probabilidade, impacto e níveis de riscos, avaliação de controles, apetite e a tolerância a riscos definidos no Plano de Gestão de Riscos do TRT7.

Art. 7º processo de GRSI deverá observar a matriz de atribuições definidas no Anexo A desta norma, sem prejuízo das competências definidas no plano de gestão de riscos institucionais, e abordará:

I - a definição do contexto da GRSI;

II - a Matriz de Gerenciamento de Riscos;

III - a elaboração do Plano de Tratamento de Riscos;

IV - a execução do Plano de Tratamento de Riscos;

V - a comunicação e a consulta;

VI - o monitoramento;

VII - a melhoria contínua.

Seção I
Da Definição do Contexto

Art. 8º Na elaboração do contexto da GRSI, sem prejuízo das disposições constantes no Plano de Gestão de Riscos do Tribunal, deverão ser observados:

I - a Política de Segurança da Informação e Comunicação do TRT7;

II - a Política de Privacidade e Proteção de Dados Pessoais do TRT7;

III - a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ);

IV - o Manual de Referência para Proteção de Infraestruturas Críticas de TIC, editado pelo CNJ, decorrente da PSEC-PJ;

V - os objetivos estratégicos, os processos de negócio e as expectativas das partes interessadas;

VI - os requisitos legais;

VII - os ativos de informação;

VIII - aefetiva participação do Comitê Gestor de Segurança da Informação;

IX - a validação da proposição do contexto pelo Comitê de Governança de TIC, antes de submetê-lo à apreciação pela Presidência.

Art. 9º O escopo da GRSI poderá abranger todos os ativos de TIC do TRT7, um segmento, um processo, um sistema, um recurso ou um ativo de informação.

Parágrafo único. É recomendado, porém, que sejam considerados prioritariamente os serviços de TIC que suportam os processos de negócio essenciais ao funcionamento do TRT7.

Seção II
Da Matriz de Gerenciamento de Riscos

Art. 10. A identificação, análise e o tratamento dos riscos de segurança da informação deverão ser elaborados com base no modelo estabelecido no Plano de Gestão de Riscos institucional e deverão conter:

I - a identificação dos ativos de TIC dentro do escopo estabelecido;

II - os riscos associados a cada ativo de TIC, considerando as ameaças envolvidas e as vulnerabilidades existentes;

III - o grau de severidade dos riscos identificados, considerando a probabilidade e as consequências da ocorrência do risco (por exemplo, comprometimento da integridade, disponibilidade, confiabilidade e/ou da autenticidade de informação) sobre os ativos de TIC envolvidos;

IV - a opção de tratamento dos riscos selecionados;

V - as ações de segurança das informações já implementadas.

§ 1º As formas de tratamento dos riscos de segurança da informação devem ser selecionadas com base:

I - no resultado do processo de avaliação de riscos;

II - no custo esperado para implantação e nos benefícios previstos;

III - nas restrições organizacionais, técnicas e estruturais; e

IV - nos requisitos legais.

§ 2º A matriz deve ser verificada e validada pelo Comitê Gestor de Segurança da Informação antes de submetê-la à apreciação do Comitê de Gestão de Riscos Institucionais.

Art. 11. Devem ser considerados para identificação do nível de risco e na priorização do tratamento, no mínimo, os seguintes critérios de avaliação:

I - o valor estratégico do processo;

II - a criticidade dos ativos;

III - o histórico de ocorrência de eventos de segurança;

IV - o valor do ativo para o processo.

Parágrafo único. Os riscos não priorizados para tratamento serão geridos de acordo com as necessidades levantadas pelas partes interessadas, pelas regulamentações e legislações vigentes e pela análise custo/benefício.

Art. 12. No processo de identificação de riscos devem ser empregados os seguintes métodos, sempre que possível:

I - ferramentas automatizadas de procura por vulnerabilidades técnicas;

II - avaliação e testes de segurança, incluindo os controles existentes;

III - testes de invasão;

IV - análise crítica de código.

Seção III
Da Elaboração do Plano de Tratamento de Riscos

Art. 13. As ações de tratamento deverão explicitar as iniciativas propostas, os responsáveis pela implementação, os recursos requeridos e o cronograma sugerido.

Parágrafo único. Cabe aos(às) gestores(as) de riscos definir, juntamente com o(a) chefe da área de segurança da informação, os planos de ação e os controles necessários para o tratamento dos riscos.

Seção IV
Da Execução do Plano de Tratamento de Riscos

Art. 14. A implementação das ações do Plano de Tratamento de Riscos, seu monitoramento e a apresentação dos resultados são de responsabilidade dos(as) gestores(as) de riscos identificados no plano de tratamento.

Seção V
Da Comunicação e da Consulta

Art. 15. Deverá ser garantida comunicação contínua para fornecer, compartilhar ou obter informações com as partes interessadas, com relação à gestão de riscos de segurança da informação e comunicação.

Seção VI
Do Monitoramento

Art. 16. Deverá ser realizado monitoramento do processo de GRSI a fim de verificar regularmente, no mínimo:

I - alinhamento às diretrizes gerais estabelecidas e às necessidades do TRT7;

II - possíveis falhas no processo ou resultados;

III - mudanças nos critérios de avaliação e aceitação dos riscos;

IV - mudanças no ambiente e/ou nos ativos de informação;

V - riscos emergentes;

VI - mudanças nos níveis de risco;

VII - implementação e eficácia dos controles.

Parágrafo único. Para cada escopo definido deverá ser apurado indicador de eficiência do plano de tratamento, de acordo com o Anexo B deste ato.

Seção VII
Da Melhoria Contínua

Art. 17. Deverá ser elaborada, anualmente, pelo Comitê de Gestão de Riscos, análise crítica com vistas ao aprimoramento contínuo da GRSI, devendo abordar, ao menos, o processo de GRSI, os resultados alcançados e as proposições de melhoria.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Art. 18. Os sistemas, serviços e os ativos de TIC homologados devem ser submetidos à unidade responsável pela Gestão de Segurança da Informação do órgão para identificação de riscos, antes de sua primeira efetiva disponibilização em ambiente de produção, de modo a se evitar a exploração de vulnerabilidades em ambiente crítico.

Art. 19. Ficam revogados:

I - o Ato TRT7.GP nº 106, de 16 de julho de 2018;

II - o Ato TRT7.GP nº 42, de 27 de março de 2020.

Art. 20. Este ato entra em vigor na data de sua publicação.

Fortaleza, 08 de junho de 2022.
REGINA GLAUCIA CAVALCANTE NEPOMUCENO
Presidente do Tribunal

ANEXO A

MATRIZ DE COMPETÊNCIAS PARA A GRSI

Etapa	Atribuição	Responsável	Aprovador	Consultado	Informados
-	Coordenar a GRSI	CGR	Presidência	CGSI	GR
-	Coordenar o Processo de GRSI	NGSI	SETIC	GR	GR
-	Disseminar cultura voltada para identificação e tratamento de riscos de segurança da informação	CGR	CGTIC	GR	GR
-	Fornecer consultoria interna em GRSI	NGSI	CGR	GR	GR CGSI
Definição do contexto	Estabelecer o contexto da GRSI	CGR	CGTIC	CGSI GR	CGSI GR
Elaboração do Plano de Tratamento de Riscos	Plano de Tratamento de Riscos de Segurança da Informação.	CGR	CGTIC e Presidência	CGSI	GR
Comunicação e Consulta	Manter as instâncias superiores informadas a respeito de todas as fases do Processo de GRSI	NGSI	SETIC	GR	CGSI; CGR

Comunicação e consulta	Manter documentação atualizada acerca da GRSI	NGSI	SETIC	GR	CGSI CGR
Monitoramento	Elaborar relatório anual quanto à efetividade do processo de GRSI.	NGSI	SETIC	GR	CGSI; CGR
Monitoramento	Monitorar e analisar periodicamente a execução do Plano de Tratamento de Riscos de Segurança da Informação	NGSI	SETIC	GR	GR, CGSI, CGR
Monitoramento	Monitorar e gerenciar os Riscos de Segurança da Informação dos ativos sob sua responsabilidade, de forma a mantê-los em um nível de exposição aceitável	GR	SETIC	-x-	SETIC, NGSI
Melhoria contínua	Avaliar periodicamente a estrutura da GRSI e propor melhorias (monitoramento e melhoria contínua)	NGSI	CGR CGTIC Presidência	CGSI GR	CGSI GR
Melhoria Contínua	Revisar o contexto da GRSI para efeito do ciclo PDCA (Plan, Do, Check, Act)	CGR	CGTIC	CGSI GR	CGSI GR

Legenda:

CGR = Comitê de Gestão de Riscos;

CGSI = Comitê Gestor de Segurança da Informação;

NGSI = Núcleo de Gestão de Segurança da Informação;

GR = Gestor(a) de Risco;

SETIC = Secretaria de Tecnologia da Informação e Comunicação;

CGTIC = Comitê de Governança de Tecnologia da Informação e Comunicação;

ANEXO B

INDICADORES

Indicador	**Índice de ativos de TI incluídos na análise de riscos**
Objetivo	Garantir que há um relatório de perfil de riscos atualizado e completo
Responsável	NGSI
Periodicidade	Anual
Origem	COBIT 5.0: Enabling process: APO12.03 Process Assessment Model ● Outcome APO12-02 ● Base pratice APO12-BP3
Fórmula	TAA / TA
Total de ativos analisados (TAA)	Quantidade de ativos críticos de TIC com análise de riscos realizada
Total de ativos (TA)	Quantidade total de ativos críticos de TIC presente no inventário
Informações complementares	Uma meta deve ser definida no estabelecimento de contexto

Indicador	**Índice de tratamento de riscos**
Objetivo	Garantir que ações de gerenciamento de risco importantes são gerenciadas e controladas
Responsável	NGSI
Periodicidade	Anual
Origem	COBIT 5.0: Enabling process: APO12.05 Process Assessment Model ● Outcome APO12-03 ● Base pratice APO12-BP5
Fórmula	SQT / QD
Soma dos coeficientes	Para cada demanda: atribuir “0” para as demandas não atendidas, “0,5”

de tratamento (SQT)	para as demandas em atendimento e “1” para as demandas atendidas
Quantidade de demandas (QD)	Quantidade de demandas propostas no plano de tratamento
Informações complementares	Uma meta deve ser definida no estabelecimento de contexto

Indicador	**Índice de Risco de Ativos**
Objetivo	Ações de gerenciamento de riscos são efetivamente implementadas
Responsável	NGSI
Periodicidade	Anual
Origem	COBIT 5.0: Enabling process: APO02.04 Process Assessment Model • Outcome APO12-04 • Base pratice APO12-BP2/BP4
Fórmula	TRA / TA
Total de ativos (TRA)	Total de ativos com risco “alto” ou maior
Total de ativos (TA)	Total de ativos críticos presentes no inventário
Informações complementares	Uma meta deve ser definida no estabelecimento de contexto Mostrar os dois cenários, índice de riscos de ativos inerente e residual após o tratamento