ANEXO 6

NSI006 – Gestão de Riscos de Tecnologia da Informação e Comunicações

(Incluído pela Portaria GP.TRT4 nº 6.137/2014 e alterado pelas Portarias GP.TRT4 nºs 7.137/2021, 6.493/2019, 4.786/2020, 2.926/2021, 299/2022 e 4.095/2023).

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TRT da 4ª Região (GRSIC-TRT4).

2. Aplicabilidade

2.1. Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRT da 4ª Região.

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. (item alterado pela Portaria nº 299/2022)

4.2. Instrução Normativa GSI/PR nº 3, 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. (alterado pela Portaria GP.TRT4 nº 299/2022)

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2019, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.4. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos. (alterado pela Portaria GP.TRT4 n° 6.493/2019)

4.5. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação; (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.6. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação; (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.7. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

4.8. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação. (incluído pela Portaria GP.TRT4 nº 4.786/2020)

5. Conceitos e definições (alterado pela Portaria GP.TRT4 nº 4.095/2023)

5.1. Ameaça - causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

5.2. Análise de riscos - processo para compreender a natureza do risco e determinar o nível de risco;

5.3. Avaliação de riscos - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;

5.4. 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;

5.5. Comunicação do risco - conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;

5.6. Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.7. Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

5.8. Evento adverso - ocorrência ou alteração negativa de um conjunto de circunstâncias;

5.9. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–TRT4) – conjunto de atividades que permitem 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;

5.10. Gestão de Riscos em Projetos de TIC – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

5.11. Gestão de Riscos em Processos de TIC – conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

5.12. Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

5.13. Impacto - é a medida do dano ocasionado caso o evento adverso concretize-se.

5.14. Probabilidade - é a possibilidade de algum evento adverso ocorrer.

5.15. Reduzir risco – forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências

negativas, ou ambas, associadas a um risco;

5.16. Reter risco – forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

5.17. Riscos de Segurança da Informação e Comunicações – 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, com impacto negativo no negócio da organização;

5.18. Transferir risco – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

5.19. Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

5.20. Vulnerabilidade - fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

6. Escopo

6.1. A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados à área de TIC, que suportam os principais processos de negócio do TRT da 4ª Região.

7. Diretrizes

7.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação deste Tribunal.

7.2. A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

7.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

8. Gestão de riscos em projetos de TIC

8.1. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Secretaria de Tecnologia da Informação de Comunicações. (alterado pela Portaria GP.TRT4 n° 6.493/2019)

9. Gestão de riscos em processos de TIC

9.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo. (alterado pela Portaria GP.TRT4 n° 7.137/2017 e pela Portaria GP.TRT4 nº 6.493/2019)

9.2. A gestão de riscos em processos de TIC é monitorada pelo Seção de Conformidade e Processos de Tecnologia da Informação e Comunicações. (alterado pela Portaria GP.TRT4 n° 2.926/2021)

10. Gestão de riscos em Segurança da Informação e Comunicações (GRSIC-TRT4) (alterado pela Portaria GP.TRT4 n° 4.786/2020)

10.1. O processo de GRSIC-TRT4 é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação.

10.2. O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018 e na Instrução Normativa GSI/PR nº 3. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

10.3. Os riscos serão avaliados a partir da: a) **Probabilidade**, que é a possibilidade de algum evento adverso ocorrer, podendo gerar impacto negativo. A escala é definida em quatro níveis: raro, possível, provável ou iminente; b) **Impacto**, que é a medida do dano ocasionado caso o evento adverso concretize-se. A escala é definida em quatro níveis: perceptível, moderado, crítico ou catastrófico. Desta forma os riscos são analisados com base em duas variáveis (probabilidade e impacto). O produto dessas duas variáveis determina o nível do risco, conforme

mapa a seguir: (alterado pela Portaria GP.TRT4 nº 4.095/2023)

	1 - Raro	2 - Possível	3 - Provável	4 - Iminente
1 - Perceptível	1	2	3	4
2 - Moderado	2	4	6	8
3 - Crítico	3	6	9	12
4 - Catastrófico	4	8	12	16

Classificação do Risco	Valores do RISCO
Muito baixo	1 a 2
Baixo	3 a 4
Médio	6 a 8
Alto	9 a 12
Muito alto	16

10.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

10.5. O processo de GRSIC-TRT4 é composto pelas etapas descritas a seguir:

10.5.1. Contextualização - compreende a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas.

10.5.2. Análise e Avaliação dos Riscos - compreende o mapeamento dos ativos, identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos.

10.5.3. Tratamento dos Riscos - compreende a implementação das ações do Plano de Tratamento de Riscos. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

10.5.4. Melhoria contínua - compreende a realização da análise crítica pela

Administração, com avaliação dos resultados e das propostas de melhoria apresentadas.

10.6. O desenho do processo de Gestão de Riscos de Segurança da Informação, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

10.7. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior.

11. Atualização da Norma

11.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.