NSI-006 – Gestão de Riscos de Tecnologia da Informação e Comunicação

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos relacionadas ao ambiente tecnológico no âmbito do Tribunal Regional Eleitoral da Bahia, aos projetos e processos de Tecnologia da Informação e Comunicação (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação do TRE-BA.

2. Aplicabilidade

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

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação, 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 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

4.2. Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01), de 15 de fevereiro de 2013, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal – APF, direta e indireta.

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.4. Norma Técnica ABNT NBR ISO 31000:2009, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.5. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

4.6. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

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

5. Conceitos e definições

5.1. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização.

5.2. Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco.

5.3. Análise/avaliação de riscos: processo completo de análise e avaliação de riscos.

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. Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

5.6. Comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas.

5.7. Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e às consequências de um risco.

5.8. 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.

5.9. Gestão de Riscos de Segurança da Informação: 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. 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.

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

5.15. 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.

5.16. 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.

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

5.18. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

6. Escopo

6.1 A Gestão de Riscos de TIC, 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 TRE-BA.

7. Diretrizes

7.1. A Gestão de Riscos de TIC deverá levar em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e estar alinhada à Política de Segurança da Informação da Justiça Eleitoral e ao Sistema de Gestão de Riscos (SGR) do Tribunal.

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

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

8. Gestão de riscos em projetos de TIC

8.1. A gestão e comunicação de riscos em projetos de TIC estão definidas na metodologia de gerenciamento de projetos do Tribunal e têm como objetivo aumentar a

probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

8.2. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos e Sistema de Gestão de Riscos do Tribunal.

8.3. A gestão de riscos em projetos deverá ser realizada pelo Gerente do Projeto e monitorada pela Seção de Gestão de Riscos e de Gerenciamento de Projetos.

9. Gestão de riscos em processos de TIC

9.1. A gestão e comunicação de riscos em processos de TIC deverão estar definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

9.2. As atividades inerentes à gestão de riscos nos processos de TIC deverão observar as diretrizes do Sistema de Gestão de Riscos do Tribunal e desta Norma.

9.3. A gestão de riscos em processos de TIC deverá ser monitorada pela Seção de Governança e de Gestão de Processos e da Qualidade.

10. Gestão de riscos de segurança da informação

10.1. O processo de gestão de riscos de segurança da informação deverá ser contínuo, fornecendo subsídios e integrando-se à implantação e operação do processo de gestão de incidentes de segurança da informação e de gestão de continuidade de negócios.

10.2. A gestão de riscos de segurança da informação deverá seguir o processo estabelecido no Sistema de Gestão de Riscos do Tribunal.