Diretoria Geral

INSTRUÇÃO NORMATIVA Nº 1, DE 15 DE FEVEREIRO DE 2024.

Dispõe sobre a gestão de riscos de segurança da informação no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das atribuições previstas no art. 19, I, da Resolução TSE n.º 23.644/2021,

CONSIDERANDO a necessidade de apoiar a gestão dos riscos de segurança da informação do TRE-RJ, cuja avaliação periódica é condição para implementação e operação do SGSI - Sistema de Gestão de Segurança da Informação da Justiça Eleitoral;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em gestão de riscos de segurança da informação previstas na norma ABNT NBR ISO/IEC 27005;

CONSIDERANDO as boas práticas em gestão da privacidade da informação previstas na norma ABNT NBR ISO/IEC 27701;

CONSIDERANDO a necessidade de gerenciar os riscos que envolvem o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD); e

CONSIDERANDO, ainda, que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio de Janeiro,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa regulamenta o processo de gestão de riscos de segurança da informação no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro - TRE-RJ, integrando a Política de Segurança de Informação da Justiça Eleitoral.

Art. 2º O processo de gestão de riscos de segurança da informação deverá estar alinhado à Política de Gerenciamento de Riscos do TRE-RJ, aplicando-se, no que couber, a metodologia de gerenciamento de riscos institucional.

Art. 3º A gestão de riscos de segurança da informação tem por objetivo a garantia da entrega de valor e o cumprimento da missão do TRE-RJ, bem como o atingimento dos objetivos estratégicos. CAPÍTULO II

DAS DEFINIÇÕES GERAIS

Art. 4° Para efeitos deste normativo, aplicam-se os termos e definições previstos na Portaria DG/TSE nº 444/2021.

Art. 5° Os riscos de segurança da informação deverão ser geridos no âmbito de cada processo, atividade ou projeto institucional, sob a responsabilidade dos respectivos gestores de riscos, apoiados pela Assessoria de Segurança da Informação - ASINFO e pelo Núcleo de Defesa Cibernética - NDEC.

Parágrafo único. Considera-se gestor de risco o magistrado ou servidor do TRE-RJ responsável por um processo, atividade ou projeto institucional, que detém autonomia administrativa em relação ao risco a ser gerenciado.

Art. 6° A gestão dos riscos de segurança da informação observará as diretrizes da norma técnica ABNT ISO/IEC 27005.

Art. 7° Todos os novos sistemas de informação, sejam estes desenvolvidos internamente, obtidos de outras instituições ou adquiridos de fornecedor externo, deverão passar por análise de riscos de segurança da informação antes de sua implementação.

CAPÍTULO III

DO ESTABELECIMENTO DE CONTEXTO

Art. 8° O estabelecimento de contexto dos riscos de segurança da informação visa à definição da abrangência da aplicação da gestão de riscos no TRE-RJ, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de avaliação e tratamento, bem como os critérios de impacto e aceitação para avaliação dos riscos.

Art. 9° Para o estabelecimento do contexto deverão ser avaliados os ambientes externo e interno, considerando-se, dentre outros, a expectativa das partes interessadas e os fatores sociais, econômicos, ambientais, humanos, tecnológicos, legais e organizacionais que se relacionam com a Justiça Eleitoral.

Art. 10. Compete à ASINFO, com o apoio da Assessoria de Gerenciamento de Riscos e Controle Interno - ASGERI, a coordenação das atividades relacionadas ao estabelecimento do contexto, que deverá ser avaliado pela Comissão de Segurança da Informação - COMSI e submetido ao(a) Diretor(a)-Geral e ao(a) Presidente, para aprovação.

CAPÍTULO IV

DO PROCESSO DE AVALIAÇÃO DO RISCO

Art. 11. O processo de avaliação dos riscos de segurança da informação compreende as seguintes etapas:

I - Identificação dos riscos - envolve a identificação: dos ativos compreendidos no contexto estabelecido e respectivos responsáveis; das ameaças que podem comprometer os ativos; dos controles existentes e planejados relacionados aos ativos; das vulnerabilidades associadas aos ativos, ameaças e controles; das consequências que uma eventual perda de confidencialidade, integridade ou disponibilidade ocasionada por uma ameaça possam causar ao cumprimento da missão institucional ou atingimento dos objetivos organizacionais; e a elaboração de uma lista de cenários de incidentes associadas aos elementos identificados anteriormente;

II - Análise dos riscos - envolve a avaliação das consequências associadas aos cenários de incidentes, de acordo com os critérios de impacto definidos no estabelecimento do contexto; a avaliação da probabilidade de ocorrência dos cenários de incidentes, levando em conta a extensão das vulnerabilidades conhecidas, os incidentes anteriores registrados e a eficácia dos controles; e a determinação do nível de risco dos cenários de incidentes;

III - Avaliação dos riscos - envolve a comparação do resultado da etapa de análise dos riscos com os critérios de aceitação dos riscos definidos no estabelecimento do contexto; e a priorização do tratamento dos riscos.

Art. 12. O desenvolvimento das etapas do processo de avaliação dos riscos será conduzido pelo gestor de riscos e comunicado à ASINFO.

CAPÍTULO V

DO TRATAMENTO E ACEITAÇÃO DOS RISCOS

Art. 13. Com base no resultado do processo de avaliação dos riscos, devem ser selecionadas, dentre as seguintes, as opções de tratamento dos riscos, a fim de que as consequências adversas sejam reduzidas ao mínimo possível:

I - modificar - compreende a inclusão, exclusão ou alteração de controles que atuem para a modificação do nível do risco;

II - reter - significa a aceitação do risco, quando o nível de risco está adequado aos critérios estabelecidos para tanto;

III - compartilhar - compreende a decisão de compartilhar o risco com um terceiro;

IV - evitar - envolve a decisão de eliminar a atividade executada pela organização que está associada ao risco ou a mudança das condições em que a atividade é executada, de forma que não fique mais exposta ao risco.

Art. 14. A proposta de tratamento dos riscos constará do Plano de Gerenciamento de Riscos, que conterá os controles e ações planejadas para o tratamento.

§ 1º O Plano de Gerenciamento de Riscos deverá ser elaborado pelo gestor de riscos e comunicado à ASINFO.

§ 2º A aceitação do risco residual que esteja além do limite dos critérios de aceitação deverá ser justificada pelo gestor de riscos e avaliada pela COMSI, com o apoio da ASINFO.

§ 3º Os riscos que permaneçam além do limite dos critérios de aceitação após a avaliação da COMSI deverão ser submetidos ao(a) Diretor(a)-Geral e ao(a) Presidente para conhecimento e deliberação.

CAPÍTULO VI

DA COMUNICAÇÃO E CONSULTA DO RISCO

Art. 15. Os riscos devem ser comunicados e compartilhados entre as partes interessadas.

§1º Os gestores de riscos devem comunicar à ASINFO os riscos identificados e avaliados e seus respectivos tratamentos.

§2º Os riscos que impactem nos objetivos institucionais deverão ser comunicados à ASGERI.

CAPÍTULO VII

DO MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS

Art. 16. O monitoramento e análise crítica dos riscos em segurança da informação deverão ser efetuados pela ASINFO e pela COMSI, por meio de acompanhamento dos planos de gerenciamento de riscos e informações compartilhadas pelos gestores de riscos.

Art. 17. Os riscos identificados devem ser reavaliados com periodicidade mínima anual.

Art. 18. Os riscos de segurança da informação devem ser monitorados, preferencialmente, por meio de solução informatizada de GRC (governança, risco e conformidade), permitindo o acesso às partes interessadas e à alta administração.

Parágrafo único. Na impossibilidade de adoção de sistema informatizado para monitoramento dos riscos devem ser adotados controles manuais, cujo controle ficará a cargo da ASINFO.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 19. O Núcleo de Defesa Cibernética e a ASINFO apoiarão os gestores de riscos quando da elaboração do processo de avaliação de riscos de segurança da informação.

Art. 20. A ASGERI dará suporte à ASINFO no desenvolvimento das práticas e instrumentos de controle para a coordenação do gerenciamento dos riscos de segurança da informação.

Art. 21. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida a COMSI ou o Comitê Gestor de Proteção de Dados Pessoais, de acordo com o tipo do risco elencado.

Art. 22. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Assessor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 23. Esta norma complementar deverá ser revisada a cada 2 (dois) anos pela ASINFO e encaminhada para nova apreciação da COMSI.

Art. 24. Esta Instrução Normativa entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.

ELINE IRIS RABELLO GARCIA DA SILVA

Diretora-Geral