INSTRUÇÃO NORMATIVA Nº 303, DE 09 DE JULHO DE 2024

Institui o Processo de Gestão de Riscos de Privacidade e Segurança da Informação do Supremo Tribunal Federal.

***O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso das atribuições que lhe confere o art. 41, inciso X, alínea b, do Regulamento da Secretaria de 2024, considerando o disposto na Resolução 773/2022, que instituiu a Política de Segurança da Informação do STF, na Resolução 759/2021, que instituiu a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do STF, na Resolução 781/2022, que instituiu a Política de Gestão de Riscos do STF, na Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), e no Processo Administrativo eletrônico 003580/2022;*

***R E S O L V E**:*

Art. 1º Fica instituído o Processo de Gestão de Riscos de Privacidade e Segurança da Informação (PGRC-PSI) do Supremo Tribunal Federal (STF).

§ 1º O PGRC-PSI é uma especialização do processo de gestão de riscos do STF e observa seus princípios, modelos e referências.

§ 2º Para os efeitos desta instrução normativa, aplica-se o glossário de termos de segurança da informação definido e publicado no Repositório Digital do STF (https://bibliotecadigital.stf.jus.br/xmlui/).

Art. 2º São objetivos do PGRC-PSI:

I – reduzir os impactos negativos que riscos em privacidade e segurança da informação podem acarretar ao STF, providenciando seu tratamento ou compreendendo e aceitando seus efeitos, de acordo com a criticidade dos ativos de informação analisados;

II – definir a estrutura, as atividades a serem realizadas, as responsabilidades e competências para a gestão de riscos de privacidade e segurança da informação no âmbito do STF.

Art. 3º O PGRC-PSI tem início com a indicação, a ser encaminhada à Coordenadoria de Integridade Digital (CIND), vinculada à Secretaria de Relações com a Sociedade (SRS), dos objetos que devem ter os seus riscos gerenciados, podendo ser originado:

I – dos titulares de unidades responsáveis pela gestão de ativos de informação;

II – dos donos dos riscos, ou seja, pessoas responsáveis por gerenciar e responder a riscos específicos associados às suas áreas de operação ou controle;

III – da própria CIND, caso verificado risco não informado pelos titulares das unidades ou pelos donos dos riscos, sendo necessária, nessa hipótese, a autorização da Alta Administração do Tribunal.

Parágrafo único. A SRS fará a consolidação das sugestões recebidas e as submeterá ao Comitê de Segurança da Informação, e, na hipótese de violação a dados pessoais, ao Comitê Executivo de Proteção de Dados, juntamente com a proposta para gestão de riscos anual.

Art. 4º Os objetos indicados nos termos do art. 3º serão identificados, analisados e avaliados nos termos da metodologia de gestão de riscos vigente no STF.

§ 1º A etapa de identificação de riscos deve se apoiar em frameworks e estruturas nacionais e internacionais de privacidade e segurança da informação para complementar técnicas de brainstorming que porventura sejam utilizadas, de forma a permitir a identificação adequada de vulnerabilidades, ameaças e controles.

§ 2º Ao final da atividade de avaliação de riscos:

I – a SRS deverá registrar, em processo sigiloso no Sistema Eletrônico de Informações (SEI), um relatório de avaliação de riscos, cujas credenciais de acesso serão concedidas apenas para os donos dos riscos, para os membros do Comitê de Segurança da Informação, para os membros do Comitê Executivo de Proteção de Dados na hipótese de violação de dados pessoais e para Alta Administração;

II – será concedido prazo para manifestação das áreas envolvidas sobre os resultados aferidos na análise de risco e apresentados no relatório elaborado pela SRS;

III – para cada risco identificado deverá ser atribuído um dono, que deve ser um gerente de processo ou o titular de uma unidade.

§ 3º O Comitê de Riscos será informado do quantitativo de riscos mapeados com a sua criticidade e o número do processo SEI.

§ 4º Os riscos também deverão ser registrados em ferramenta informatizada específica.

§ 5º A qualquer tempo, os membros do Comitê de Segurança da Informação e do Comitê Executivo de Proteção de Dados poderão ter acesso ao painel de riscos, a ser disponibilizado em ferramenta informatizada, bem como às manifestações das áreas envolvidas, registradas no processo SEI.

Art. 5º A SRS irá elaborar, em conjunto com as áreas envolvidas, o Plano de Tratamento de Riscos, onde estarão descritas as opções disponíveis para a mitigação dos riscos identificados, bem como a informação de quais seriam as soluções indicadas pelas áreas.

Parágrafo único. A mitigação de riscos de privacidade e segurança da informação pode envolver a implementação de melhorias em processos e/ou projetos, ou a aquisição de ferramentas e soluções.

Art. 6º A seleção de controles de privacidade e segurança da informação deve ser realizada observando a melhor relação risco/retorno em sua implementação.

Art. 7º Os controles implementados permitirão aferir a maturidade em privacidade e segurança da informação do Tribunal, levando em consideração:

I – a dimensão política do controle;

II – a dimensão de abrangência da implementação do controle;

III – a dimensão de automatização da implementação do controle;

IV – a dimensão de comunicação entre as três linhas, conforme o modelo das três linhas do Institutos dos Auditores Internos - IIA.

Parágrafo único. A aferição da maturidade dos controles em privacidade e segurança da informação deverá ser realizada, no mínimo, uma vez ao ano, pela SRS.

Art. 8º Compete ao Gestor de Segurança da Informação e ao Encarregado pelo Tratamento de Dados Pessoais a coordenação do disposto nesta instrução normativa.

Art. 9º A SRS monitorará os riscos, reavaliando-os, no mínimo, a cada 12 meses.

Art. 10. Fica revogada a Instrução Normativa 283, de 11 de julho de 2023.

Art. 11. Esta instrução normativa entra em vigor na data de sua publicação.

EDUARDO S. TOLEDO

Publicado no DJE/STF em 10/7/2024.