Boletim de Serviço Eletrônico do STF em 14/07/2023

SUPREMO TRIBUNAL FEDERAL

INSTRUÇÃO NORMATIVA Nº 283, DE 11 DE JULHO DE 2023.

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

O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL, no uso da atribuição que lhe confere o art. 28, IX, *b*, do Regulamento da Secretaria, e considerando o disposto na Resolução nº 773/2022, que instituiu a Política de Segurança da Informação do STF, na Resolução nº 781/2022, que instituiu a Política de Gestão de Riscos do STF, e no Processo Administrativo eletrônico n° 003580/2022,

R E S O L V E:

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

§ 1º O PGRC-SI 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 na página da Assessoria de Segurança da Informação (ASI) na Intranet do STF.

Art. 2º São objetivos do PGRC-SI:

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

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

Art. 3º O PGRC-SI terá início com a indicação dos objetos que devem ter os seus riscos gerenciados, podendo ser originado pelo:

I – titular de unidade responsável pela gestão de ativos de informação;

II – gestor dos riscos já mapeados para reavaliação; e

III – titular da ASI, após submissão de pedido à unidade responsável pelo ativo de informação e autorização do respectivo titular.

§ 1° No caso do disposto nos incisos I e II, as indicações serão encaminhadas à ASI.

§ 2º A ASI fará a consolidação das indicações recebidas e as submeterá ao Comitê de Segurança da Informação (CSI/STF), com a proposta para o plano anual de gestão dos riscos da segurança da informação.

Art. 4º Os objetos indicados nos termos do art. 3º serão identificados, analisados e avaliados conforme a metodologia prevista no Guia de Gestão de Riscos do STF.

§ 1º A etapa de identificação de riscos considerará, principalmente, *frameworks* e estruturas nacionais e internacionais de segurança da informação, além de técnicas de *brainstorming* que porventura sejam utilizadas para complementá-las.

§ 2º Ao final da atividade de avaliação de riscos, a ASI elaborará relatório, a ser registrado em processo eletrônico, e adotará as seguintes ações:

I – atribuirá um gestor para cada risco, que deve ser gerente de processo ou titular de unidade;

II – concederá credenciais de acesso apenas aos gestores do risco, aos membros do CSI/STF e à Alta Administração; e

III – concederá prazo para manifestação das áreas envolvidas sobre os resultados aferidos na análise de risco apresentados no relatório.

Art. 5º Os riscos serão registrados em ferramenta informatizada específica mantida pela ASI, disponível a qualquer tempo aos membros do CSI/STF e à Alta Administração.

Art. 6º O Comitê de Riscos (CR-STF) será informado do quantitativo de riscos mapeados e as criticidades.

Art. 7º A ASI elaborará, em conjunto com as áreas envolvidas, o Plano de Tratamento de Riscos, em que estarão descritas as opções disponíveis para a mitigação dos riscos identificados, bem como as soluções indicadas pelas áreas.

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

Art. 8° A maturidade em segurança da informação do Tribunal será aferida por meio dos controles que serão implementados para tratamento dos riscos.

Parágrafo único. Os controles utilizados para aferição da maturidade, bem como a metodologia, serão definidos, anualmente, pelo CSI/STF.

Art. 9º A aferição da maturidade em segurança da informação, no que tange aos controles relacionados à tecnologia da informação, deverá ser realizada, no mínimo, uma vez ao ano, pela Secretaria de Tecnologia da Informação, com o acompanhamento da ASI.

Art. 10. A ASI monitorará os riscos, reavaliando-os, no mínimo, a cada 12 (doze) meses.

Art. 11. Compete ao Gestor de Segurança da Informação a coordenação do disposto nesta Instrução Normativa.

Art. 12. Esta Instrução Normativa entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Miguel Ricardo De Oliveira Piazzi**, **DIRETOR-GERAL**, em 14/07/2023, às 17:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sistemas.stf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2264371** e o código CRC **0DF6B93F**.