INSTRUÇÃO NORMATIVA Nº 304, DE 09 DE JULHO DE 2024

Altera a Instrução Normativa 267, de 12 de maio de 2022, que institui o Processo de Gestão de Incidentes de 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 Política de Segurança da Informação do STF e o que consta do Processo Administrativo eletrônico 004814/2021,*

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

Art. 1º O art. 1º; o art. 2º; os §§ 1º e 2º do art. 5º; o inciso II do art. 7º; o art. 8º; os §§ 1º e 2º do art. 9º; o art. 11; o inciso V do art. 12; o art. 15; o art. 16; a alínea b do inciso II, a alínea a do inciso III e o parágrafo único do art. 17; e o art. 20 da Instrução Normativa 267, de 12 de maio de 2022, passam a vigorar com a seguinte redação:

"Art. 1º .....

Parágrafo único. O GISI aplica-se também a incidentes de segurança relacionados à proteção de dados, na forma da Lei 13.709/2018 (LGPD)." (NR)

"Art. 2º Para os efeitos deste normativo e de suas regulamentações, aplicar-se-á glossário de termos de segurança da informação definido e publicado no Repositório Digital do STF (https://bibliotecadigital.stf.jus.br/xmlui/)." (NR)

"Art. 5º A Coordenadoria de Segurança Cibernética da Secretaria de Tecnologia e Inovação (CSEC/STI) tem a responsabilidade de receber, analisar, classificar, tratar e reportar os incidentes, além de gerar insumos para o Comitê de Segurança da Informação e para o Comitê Executivo de Proteção de Dados para tomada de ações ou decisões gerenciais e ainda:

.....

§ 1º A CSEC/STI deve ser constantemente treinada, equipada e capacitada nos serviços que serão executados para que possa identificar o maior número possível de incidentes que poderão ocorrer no ambiente do STF e atuar no processo de GISI.

§ 2º À CSEC/STI cabe desempenhar o papel da Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR), conforme as normas que regulam o tema na Administração Pública." (NR)

"Art. 7º .....

.....

II - internas: recebidas de colaboradores que utilizam a rede do STF, podendo ser detectadas pelas ferramentas de monitoramento dos ativos de informação do Tribunal ou encaminhadas via Service Desk ou contato direto com membros da CSEC/STI." (NR)

"Art. 8º O registro consiste em cadastrar o incidente de segurança reportado no sistema JIRA e acionar a CSEC/STI para fazer a triagem e análise da notificação." (NR)

"Art. 9º .....

§ 1º A CSEC/STI deve ter previamente definida a equipe de triagem que será acionada para analisar cada tipo de incidente de segurança da informação.

§ 2º Após o registro, o evento é encaminhado à equipe de triagem, que irá verificar se realmente é um incidente de segurança e se deverá ser tratado pela CSEC/STI." (NR)

"Art. 11. A CSEC/STI deve basear a classificação dos incidentes por meio da severidade do evento ocorrido, sendo que para cada nível deverão ser adotadas ações específicas." (NR)

"Art. 12. .....

.....

V - muito baixo: incidente originário em atividades ou ativos que possuem contingenciamento ou baixa relevância e que deve ser monitorado de acordo com a fila de priorização de incidentes, podendo o tratamento ser realizado por equipes técnicas externas, com acompanhamento da CSEC/STI." (NR)

"Art. 15. Para definir os tipos de tratamento nos quais a CSEC/STI atuará, deverão ser adotadas as melhores práticas, a exemplo das recomendações do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov), com o objetivo de uniformizar os tipos de incidentes do STF com os padrões existentes mundialmente." (NR)

"Art. 16. A CSEC/STI deve definir e manter uma listagem com a tipificação dos incidentes que serão tratados." (NR)

"Art. 17. .....

.....

II - .....

.....

b) registro de informação relevante sobre o incidente e recomendações para mitigação no sistema JIRA e para o controle de incidentes pela CSEC/STI;

III - .....

a) acionar o plano de continuidade de negócios, na eventualidade de existir a necessidade de restauração do ambiente, com a definição da equipe responsável pelo processo de restauração, que poderá ou não conter os integrantes da CSEC/STI envolvidos no processo de resposta a incidentes;

.....

Parágrafo único. Para a troca de informações sobre o tratamento do incidente, deve ser utilizado o canal de informação oficial definido pelo Coordenador da CSEC/STI, com a presença apenas dos especialistas da área, membros e demais servidores diretamente envolvidos no tratamento dos incidentes." (NR)

"Art. 20. O detalhamento técnico dos produtos gerados dentro do processo de resposta a incidentes e os procedimentos detalhados de acordo com cada tipo de incidente devem ser fornecidos e atualizados periodicamente pela CSEC/STI." (NR)

Art. 2º Fica acrescido o art. 6º-A à Instrução Normativa 267/2022:

"Art. 6º-A O Comitê Executivo de Proteção de Dados (CEPD) e o Encarregado pelo Tratamento de Dados Pessoais devem ser prontamente informados sobre incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais.

§ 1º Compete ao CEPD comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular nos termos do art. 48 da Lei nº 13.709/2018. Essa comunicação deve incluir detalhes claros sobre:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo." (NR)

Art. 3º Esta instrução normativa entra em vigor na data de sua publicação.

EDUARDO S. TOLEDO

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