Boletim de Serviço Eletrônico do STF em 18/05/2022

SUPREMO TRIBUNAL FEDERAL

INSTRUÇÃO NORMATIVA Nº 267, DE 12 DE MAIO DE 2022.

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 da atribuição que lhe conferem os artigos 28, IX, "b", e 108-A, X, do Regulamento da Secretaria, 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 Fica instituído o Processo de Gestão de Incidentes em Segurança da Informação (GISI) do Supremo Tribunal Federal (STF).

Art. 2º Para os efeitos deste normativo e de suas regulamentações, aplicar-se-á o glossário de termos de segurança da informação definido e publicado na intranet do STF.

Art. 3º O Processo de GISI corresponde ao conjunto de medidas que são aplicadas, de forma cíclica, possibilitando a resolução de incidentes em segurança da informação, minimizando o impacto do incidente através da contenção até a recuperação do ativo comprometido, acompanhado de monitoramento e comunicação com as partes envolvidas.

Art. 4º São etapas do Processo de GISI:

I - recebimento;

II - registro;

III - análise;

IV - classificação;

V - tratamento; e

VI - realização de melhorias no processo cíclico.

§ 1º A comunicação e o monitoramento são atividades que devem ser realizadas em cada etapa do processo, de acordo com suas particularidades.

§ 2º O processo é cíclico, envolvendo uma série de medidas que são repetidamente aplicadas até o incidente ficar totalmente resolvido e todas as partes envolvidas terem as informações necessárias relacionadas ao incidente.

Art. 5º O Núcleo de Prevenção, Tratamento e Resposta a Incidentes em Segurança da Informação do Supremo Tribunal Federal (NPTRI/STF) tem a responsabilidade de receber, analisar, classificar, tratar e reportar os incidentes, além de gerar insumos para o Comitê de Segurança da Informação para tomada de ações ou decisões gerenciais e ainda:

I - armazenar os registros para formação de bases de conhecimento históricas a partir dos incidentes tratados;

II - emitir relatórios acerca de notificações e/ou incidentes para o Gestor de Segurança da Informação;

III - manter um processo de comunicação contínua, de forma a permitir que as informações relevantes sobre o incidente sejam repassadas, sempre que necessário, às partes interessadas.

§ 1º O NPTRI deve ser constantemente treinado, equipado e capacitado 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 As atividades do NPTRI equivalem às atividades desempenhadas pela Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR), conforme as normas que regulam o tema na Administração Pública.

Art. 6º O Comitê de Segurança da Informação (CSI) deve ser alertado sempre que ocorrer incidentes classificados como de gravidade elevada ou crítica.

Parágrafo único. O Tribunal deve atuar para minimizar o impacto do incidente através da contenção até a recuperação do impacto causado, de acordo com a classificação do incidente.

Art. 7º A etapa de recebimento é realizada mediante notificações:

I - externas: recebidas via e-mail (si@stf.jus.br), ofício ou demais comunicados de origem externa ao Tribunal;

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 do NPTRI.

Art. 8º O registro consiste em cadastrar o incidente de segurança reportado no sistema JIRA e o NPTRI deve ser acionado para fazer a triagem e análise da notificação.

Art. 9º A análise é o procedimento realizado para verificar se o evento reportado é ou não um incidente de segurança da informação.

§ 1º O NPTRI 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 pelo NPTRI.

§ 3º Caso o evento reportado não seja identificado como um incidente em segurança da informação, este será encerrado como notificação e as partes interessadas serão comunicadas.

§ 4º No caso de confirmação do incidente, este será classificado de acordo com as normas contidas na etapa classificar.

Art. 10. A etapa de classificação tem o objetivo de identificar o grau de severidade do incidente.

Art. 11. O NPTRI deve basear a classificação dos incidentes por meio da severidade do evento ocorrido, sendo que para cada nível deverão ser adotadas ações específicas.

Art. 12. Os níveis de severidade com as respectivas ações são os seguintes:

I - crítico: incidente com dano potencial de inviabilização completa das atividades do órgão e que deve ser tratado imediatamente, através de mobilização integral das equipes responsáveis;

II - elevado: incidente com dano potencial de inviabilização parcial das atividades do órgão e deve ser tratado imediatamente, com a mobilização parcial das equipes responsáveis ao tipo de evento;

III - moderado: incidente que pode afetar parte da organização, causando atrasos ou retrabalho, não trazem danos significativos, se tratados a tempo e deve ser monitorado e tratados de acordo com a fila de priorização de incidentes existente, com comunicação tempestiva aos responsáveis;

IV - baixo: incidente que impacta as atividades ou ativos secundários do STF, não trazem danos significativos, se tratados a tempo, e deve ser monitorado e tratado de acordo com a fila de priorização de incidentes existente, com comunicação tempestiva aos responsáveis;

V - muito baixo: incidente originário em atividades ou ativos que possuem contingenciamento ou baixa relevância e deve ser monitorado de acordo com a fila de priorização de incidentes, podendo o tratamento ser realizado por equipes técnicas externas, com acompanhamento do NPTRI.

Art. 13. Caso a severidade do incidente seja classificada como crítica ou elevada, o CSI deve ser comunicado, para apoio e recomendações de tratamento.

Art. 14. Na etapa de classificação também é definido o tipo do incidente, de forma a auxiliar no correto encaminhamento às equipes envolvidas para o tratamento.

Art. 15. Para definir os tipos de tratamento que o NPTRI atuará, podem ser utilizadas as recomendações do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov) e as melhores práticas, tendo como objetivo padronizar os tipos de incidentes do STF com os padrões existentes mundialmente.

Art. 16. O NPTRI deve definir e manter uma listagem com a tipificação dos incidentes que serão tratados.

Art. 17. O tratamento investiga o incidente a fim de identificar a causa raiz e possíveis meios para reduzir os impactos no órgão e segue as seguintes fases:

I - contenção: tem como objetivo principal limitar o dano e prevenir qualquer dano posterior, com as seguintes providências:

a) preservação de evidências, de acordo com as normas vigentes no Tribunal;

b) análise de ações de curto e médio prazo que deverão ser tomadas;

II - erradicação: busca tratar os sistemas afetados, com as seguintes providências:

a) eliminação das causas e o incremento na segurança;

b) registro de informação relevante sobre o incidente e recomendações para mitigação no sistema JIRA, para o controle de incidentes pelo NPTRI;

III - restauração: busca restabelecer os recursos afetados para um estado íntegro e disponível, com o cuidado para garantir que não levará a outros incidentes, com as seguintes providências:

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 componentes do NPTRI envolvidos no processo de resposta a incidentes;

b) acionar o protocolo de gerenciamento de crise em conjunto com um plano de continuidade de negócios, caso seja verificado que o incidente não será rapidamente mitigado, que poderá causar dano material ou à imagem do Tribunal, afetar uma atividade finalística e/ou atrair a atenção da mídia.

Parágrafo único. Deve ser utilizado o canal de informação oficial definido pelo Supervisor do NPTRI para a troca de informações sobre o tratamento do incidente, com a presença apenas dos especialistas da área, membros e demais servidores diretamente envolvidos no tratamento dos incidentes.

Art. 18. Na melhoria as lições aprendidas devem ser documentadas e compartilhadas com as equipes envolvidas, descrevendo formas de obter melhores resultados e reavaliando riscos para evitar novos incidentes.

Art. 19. As etapas de comunicação e monitoramento ocorrem durante todo o ciclo de vida do incidente.

§ 1º A ferramenta JIRA deve ser alimentada de forma a possibilitar a comunicação e monitoramento dos incidentes com as partes interessadas, em especial dos incidentes classificados como críticos ou elevados e será o recurso para comunicação interna do incidente.

§ 2º O CSI definirá previamente o servidor responsável para elaboração de informes, notas ou equivalentes junto à Secretaria de Comunicação do Tribunal, de acordo com a Política de Comunicação Social do STF.

Art. 20. O detalhamento técnico dos produtos produzidos dentro do processo de resposta a incidentes e os procedimentos detalhados de acordo com cada tipo de incidente devem ser fornecidos e atualizados periodicamente pelo NPTRI.

Art. 21. Esta Instrução Normativa entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Edmundo Veras Dos Santos Filho**, **DIRETOR-GERAL**, em 18/05/2022, às 15:02, 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 **1873484** e o código CRC **93F1397A**.

004814/2021 1873484v6