Boletim de Serviço Eletrônico em 30/11/2021

CONTROLADORIA-GERAL DA UNIÃO

PORTARIA Nº 2806/2021

PORTARIA Nº 2806, DE 29 DE NOVEMBRO DE 2021

Estabelece outras atividades e atribuições complementares necessárias ao desempenho da atuação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Controladoria-Geral da União.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA CONTROLADORIA-GERAL DA UNIÃO, no uso das atribuições que lhe confere o disposto no art. 8º do Anexo I ao Decreto nº 9.681, de 3 de janeiro de 2019, e em observância à delegação que lhe foi conferida no art. 13 da Portaria SE/CGU nº 1.497, de 21 de junho de 2021, resolve:

Art. 1º Esta Portaria estabelece outras atividades e atribuições complementares necessárias ao desempenho da atuação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Controladoria-Geral da União - ETIR-CGU e demais envolvidos no tratamento de incidentes de segurança cibernética, de acordo com a Norma Complementar nº 05/IN01/DSIC/GSIPR, a Norma Complementar nº 08/IN01/DSIC/GSIPR, a Norma Complementar nº 21/IN01/DSIC/GSIPR e a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

Art. 2º As políticas a serem observadas pela ETIR-CGU estabelecem que:

I - todo suposto incidente de segurança cibernético será registrado e analisado; e

II - todo incidente de segurança cibernético constatado será registrado, tratado, encerrado e comunicado.

Art. 3º A ETIR-CGU possui autonomia para executar os processos de tratamento e resposta aos incidentes cujo impacto e procedimentos de recuperação

já sejam de conhecimento da própria equipe e desde que as medidas de tratamento não interrompam a disponibilidade dos sistemas ou dos serviços da CGU.

Art. 4º O tratamento de incidentes que não se enquadram no art. 3º deverá seguir o processo de Gestão de Mudanças para avaliação e implementação da solução.

Art. 5º As atividades executadas pela ETIR-CGU e demais envolvidos no tratamento de incidentes de segurança cibernética devem estar alinhadas com o Processo "Gerenciar Incidentes de Segurança Cibernética", publicado na Base de Conhecimento da CGU.

Art. 6º Compete ao Agente Responsável:

I - coordenar as atividades da ETIR-CGU e acompanhar os eventos de tratamento dos incidentes;

II - assegurar a participação dos servidores no apoio à equipe ETIR-CGU, nos casos em que o tratamento dos incidentes exigir conhecimentos multidisciplinares e a equipe não possuir autonomia para resolução;

III - criar e manter a documentação dos procedimentos internos atualizados;

IV - comunicar ao Gestor de Segurança da Informação as ocorrências de incidentes;

V - comunicar ao Encarregado dos Dados da CGU sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares e prover as informações necessárias para que o mesmo atue junto a ANPD e titulares dos dados;

VI - interagir com as áreas internas da CGU e órgãos externos a fim de assegurar a execução das atividades do Processo de Gerenciamento de Incidentes Cibernéticos;

VII - emitir alertas e advertências, bem como disseminar experiências e informações relacionadas à segurança por meio de campanhas de segurança da informação;

VIII - apoiar na proposição de normativos ou novos requisitos de infraestrutura ou procedimentos internos relacionados à segurança da informação e tratamento de incidentes cibernéticos;

IX - apresentar, quando solicitado, os resultados das atividades da ETIR-CGU ao Gestor de Segurança da Informação e Comitê Gerencial de Segurança Corporativa - CGSC;

X - informar ao Gestor de Segurança da Informação sobre a necessidade da adoção de procedimentos legais, cíveis, disciplinares ou administrativos em razão da existência de indícios de ilícitos criminais, abuso ou negligência no incidente cibernético; e

XI - avaliar histórico de incidentes e contribuir com sugestões de melhorias.

Art. 7º Compete aos integrantes da ETIR-CGU:

I - analisar as suspeitas de incidentes cibernéticos;

II - realizar o tratamento de incidentes cibernéticos e das vulnerabilidades;

III - emitir alertas e advertências ao Agente Responsável;

IV - apoiar na disseminação de experiências e informações relacionadas à segurança;

V - prospectar e monitorar novas tecnologias;

VI - detectar intrusão em redes de computadores;

VII - apoiar a elaboração e a revisão de normativos relacionados à segurança da informação e tratamento de incidentes cibernéticos;

VIII - executar as atividades em conformidade com o Processo de Gerenciamento de Incidentes cibernéticos, disponibilizado na Base do Conhecimento;

IX - priorizar a continuidade dos serviços corporativos observando a Política de Segurança da Informação - POSIN da CGU;

X - manter o registro de todos os incidentes cibernéticos notificados ou detectados, assegurando a manutenção do histórico das atividades da ETIR-CGU e possibilitando a geração dos seguintes relatórios:

a) Relatório de Comunicação de Incidentes de Segurança em Redes Computacionais (modelo exemplificado no anexo A da NC nº 21/IN01/DSIC/GSIPR; e

b) Relatório sobre incidente de segurança com dados pessoais, contendo informações conforme orientações da ANPD (www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

XI - manter o Agente Responsável atualizado sobre as ocorrências de incidentes de segurança, envolvendo ou não dados pessoais, e detecção de indícios de ilícitos criminais;

XII - avaliar os resultados do tratamento de incidentes de segurança e elaborar o Relatório de Incidentes após a finalização do tratamento dos incidentes;

XIII - manter as evidências dos incidentes detectados preservadas e, em caso de impossibilidade de preservação das mídias afetadas, registrar o problema e os procedimentos adotados na ferramenta ITSM;

XIV - preencher, quando couber, o Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança (modelo exemplificado no anexo B da NC nº 21/IN01/DSIC/GSIPR); e

XV - realizar a triagem de todas as notificações suspeitas de incidentes recebidas por meio da ferramenta ITSM ou do canal "abuse@cgu.gov.br" e proceder com o registro das Requisições de Incidentes para os casos de incidentes confirmados.

Art. 8º Compete ao Gestor de Segurança da Informação, designado pelo art. 10 da Portaria SE/CGU nº 947, de 27 de abril de 2021:

I - aprovar o processo de criação e gestão da ETIR-CGU;

II - acompanhar as ações realizadas pela ETIR-CGU;

III - apoiar a implementação, a manutenção e o fornecimento da infraestrutura necessária à ETIR-CGU;

IV - comunicar as autoridades competentes do órgão sobre incidentes de segurança relevantes e de impacto nas atividades primordiais da CGU; e

V - solicitar o envolvimento de outras áreas diversas a DTI ou outros órgãos em investigação e solução de incidentes de segurança da informação.

Art. 9º Esta Portaria observará, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de

18 de outubro de 2021.

Art. 10. Esta Portaria entra em vigor na data da sua publicação.

HENRIQUE APARECIDO DA ROCHA

Documento assinado eletronicamente por **HENRIQUE APARECIDO DA ROCHA**, **Diretor de Tecnologia da Informação**, em 29/11/2021, às 17:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 2193838 e o código CRC 3DE1E8D0

Referência: Processo nº 00190.109274/2021-14 SEI nº 2193838