# SEÇÃO I – ATOS NORMATIVOS

## ATOS DO DIRETOR DO CENTRO NACIONAL DE MONITORAMENTO E ALERTAS

## PORTARIA CEMADEN Nº 288, DE 1º DE JULHO DE 2022

*Dispõe sobre instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes de Computadores – ETIR no CEMADEN.*

**O DIRETOR** do Centro Nacional de Monitoramento e Alertas de Desastres Naturais – CEMADEN, nomeado por meio da Portaria nº 998, de 3 de junho de 2015, publicada na Seção 2, do DOU nº 105, dia 5 de junho de 2015, apostilada pela Portaria nº 5197 /2016/SEI-MCTIC, de 14 de novembro de 2016, publicada no Boletim de Serviço nº 21-A, de 14 de novembro de 2016, reconduzido por meio da Portaria nº 15, de 2 de janeiro de 2020, publicada na Seção 2, do DOU nº 03, dia 6 de janeiro de 2020, no uso de suas competências e considerando o Decreto nº 10.748, de 16 de julho de 2021; o Decreto nº 9.637, de 26 de dezembro de 2018; a Portaria nº 201/2021/SEI-CEMADEN, de 16 de setembro de 2021; a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020; a Instrução Normativa GSI/PR nº 02 de 24 de julho de 2020; a Norma Complementar nº 05 /IN01/DSIC/GSIPR, de 17 de agosto de 2009; e a Norma Complementar nº 08 /IN01/DSIC/GSIPR, de 24 de agosto de 2010, **RESOLVE:**

**Art. 1º. Designar** Marcus Vinícius Salgado Mendes, Tecnologista - DIPIN/CGPDE, e Eduardo Fávero Pacheco da Luz, Tecnologista - DIPIN/CGPDE, para, sob a presidência do primeiro, como Agente Responsável, e a vice-presidência do segundo, comporem a Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes de Computadores – ETIR do CEMADEN, para atuar na prevenção, tratamento e resposta a incidentes na rede de computadores deste Centro.

**Art. 2º.** Caberá à ETIR planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do CEMADEN.

**Art. 3º.** A ETIR/CEMADEN prestará os seguintes serviços:

**I -** Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

**II -** Tratamento de Artefatos Maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa.

**III -** Tratamento de Vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

**IV -** Emissão de Alertas e Advertências: serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.

**Art. 4º**. O modelo de implementação adotado pela ETIR/CEMADEN é o Modelo 1 proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, que prevê a composição da equipe por membros da área de Tecnologia da Informação – TI, integrantes da Divisão de Desenvolvimento de Produtos Integrados (DIPIN), que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes em redes computacionais.

**Art. 5º.** A ETIR/CEMADEN terá autonomia compartilhada, recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça, destacando as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não sejam seguidas.

**Art. 6º.** A comunicação dos incidentes de segurança em rede de computadores à ETIR/CEMADEN será feita por meio do endereço etir@cemaden.gov.br.

**Art. 7º.** Esta Portaria entre em vigor na data de sua publicação.

**OSVALDO LUIZ LEAL DE MORAES**

Diretor