Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 121 - DOU – 29/06/22 - Seção 1 – p.101

Ministério da Educação
Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

PORTARIA Nº 110, DE 21 DE JUNHO DE 2022

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

A PRESIDENTE DA COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR, no uso das atribuições que lhe foram conferidas pelo art. 26, incisos II e IX do Estatuto aprovado pelo Decreto nº 8.977, de 30 de janeiro de 2017, com fundamento no art. 12 do Decreto nº 10.748, de 16 de julho de 2021; no art. 15, inciso IV, combinado com o art. 16, inciso III, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 e suas alterações; na Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009; na Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010; e na Política de Segurança da Informação e Comunicações - PoSIC da CAPES, instituída pela Portaria GAB nº 199, de 29 de agosto de 2019, e demais informações que constam do processo n.° 23038.005031/2022-49, resolve:

Art. 1º Esta Portaria dispõe sobre a recriação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da CAPES, define suas competências, composição, regras de funcionamento e deliberação, bem como sua duração e objetivos, além de tratar sobre os procedimentos para o gerenciamento de incidentes cibernéticos nesta Fundação.

Art. 2º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da CAPES fica recriada, na forma do art. 6º do Decreto nº 9.759, de 2019, e passa a reger-se pelas disposições deste ato.

Competências

Art. 3º Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos:

I - receber, analisar, filtrar, classificar, responder solicitações, alertas e notificações de incidentes cibernéticos nos ativos de informação da CAPES;

II - implementar um modelo de gestão de incidentes;

III - realizar controle dos incidentes cibernéticos;

IV - elaborar iniciativas relacionadas à prevenção de incidentes cibernéticos;

V - recuperar sistemas;

VI - analisar intrusões;

VII - cooperar com outras equipes de prevenção, tratamento e resposta a incidentes cibernéticos;

VIII - participar de fóruns e redes nacionais e internacionais; e

IX - comunicar imediatamente o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados pela CAPES.

Composição e Coordenação

Art. 4º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos compõe-se dos seguintes membros:

I - o chefe da Divisão de Administração de Redes, que a coordenará; e

II - o chefe da Divisão de Suporte ao Usuário.

§ 1º Nas ausências e impedimentos legais, os titulares serão representados por seus substitutos legais, com as mesmas atribuições.

§ 2º Preferencialmente, a composição dos membros será feita por administradores de rede ou de sistema ou, ainda, por especialistas em segurança.

Art. 5º O Chefe da Divisão de Administração de Redes será o coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, incumbido de organizar as atividades da Equipe, especialmente no que concerne ao respeito às normas estabelecidas neste ato e à consecução da missão a ela atribuída.

Art. 6º São atribuições do Coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos:

I - coordenar a implantação e manutenção da Equipe;

II - interagir com outras Equipes;

III - garantir a existência de meios e procedimentos para registro, comunicação dos incidentes cibernéticos e seu tratamento;

IV - repassar ao Gestor de Segurança da Informação e Comunicação da CAPES informações sobre as atividades da Equipe;

V - acionar as autoridades competentes, preservar evidências e manter cadeia de custódia, no caso de indícios criminais; e

VI - envolver, quando necessário ao tratamento de incidentes, colaboradores das demais unidades da CAPES.

Art. 7º São atribuições dos membros da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos:

I - definir metodologia e documentar procedimentos relacionados ao tratamento e resposta a incidentes cibernéticos;

II - auxiliar o Coordenador na tomada de decisões;

III - investigar as vulnerabilidades e as causas dos incidentes cibernéticos;

IV - implementar mecanismos que visem controles dos incidentes de cibernéticos e/ou indicar necessidade de melhoria;

V - garantir a confidencialidade das informações tratadas;

VI - registrar adequadamente os incidentes cibernéticos.

Missão, Público-Alvo, Modelo de Implementação, Estrutura Organizacional, Autonomia e Serviços

Art. 8º A missão da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos instituída por esta Portaria é a facilitação e a coordenação das atividades de tratamento e resposta a incidentes cibernéticos na CAPES, além de prestar serviços relacionados à segurança cibernética, em observância à Política de Segurança da Informação e Comunicações - PoSIC e aos processos de gestão de riscos de Segurança da Informação e Comunicação - SIC da Instituição.

Art. 9º Os serviços prestados pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos recaem sobre os ativos de informação da CAPES.

Parágrafo único. Inclui-se no conceito de ativos da informação, dentre outros, toda e qualquer informação, pessoa, software, hardware, serviços e bens, tangíveis ou intangíveis, que tenham valor, ainda que não patrimonial, para a CAPES.

Art. 10. O modelo de implementação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será o "Modelo 1 - Utilizando a equipe de Tecnologia da Informação - TI", descrito na Norma Complementar nº 05/IN01/DSIC/GSIPR, item 7.1, do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, o que significa que os membros da Equipe, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes cibernéticos na CAPES.

Art. 11. Para o cumprimento de suas atribuições, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES poderá trocar informações com outras equipes e organismos de tratamento de incidentes, a exemplo do CTIR Gov.

Art. 12. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será supervisionada pela Diretoria de Tecnologia da Informação - DTI, na pessoa do Gestor de Segurança da Informação e Comunicações da CAPES.

Parágrafo único. A DTI será responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover o apoio administrativo necessário ao pleno exercício de suas atividades.

Art. 13. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos tem autonomia para realizar as ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança.

Parágrafo único. Durante um incidente de segurança, se tal se justificar, o Coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos poderá tomar unilateralmente a decisão de executar as medidas de tratamento, devendo submetê-las aos demais, para convalidação, na próxima convocação do colegiado.

Art. 14. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos deve implementar os seguintes serviços:

I - tratamento de incidentes cibernéticos, 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;

III - tratamento de vulnerabilidades;

IV - emissão de alertas e advertências;

V - anúncios;

VI - prospecção ou monitoração de novas tecnologias;

VII - avaliação de segurança;

VIII - desenvolvimento de ferramentas de segurança;

IX - detecção de intrusão; e

X - disseminação de informações relacionadas à segurança.

Parágrafo único. As atividades executórias relativas aos serviços acima poderão ser realizadas por meio de prestadores de serviços contratados pela CAPES, sob a supervisão da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Duração e apresentação de resultados

Art. 15. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos tem caráter permanente.

Art. 16. Todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Art. 17. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos apresentará relatórios semestrais ao Gestor de Segurança da Informação e Comunicação da CAPES, em que faça constar as atividades desenvolvidas e os resultados até então obtidos.

Reuniões

Art. 18. As reuniões realizar-se-ão, ordinariamente, bimestralmente ou extraordinariamente, quando convocadas pelo coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Art. 19. As convocações para reuniões da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, promovidas com antecedência mínima de 5 (cinco) dias, especificarão data, local de realização e o horário de início e o horário limite de término da reunião.

Art. 20. As reuniões poderão ser presenciais ou virtuais, convocadas pelo coordenador da equipe, vedando-se o custeio de deslocamentos pela CAPES.

Art. 21. Para a realização da reunião é obrigatória a presença de todos os membros da equipe.

Art. 22. As decisões da equipe serão tomadas por unanimidade.

Parágrafo único: Em caso de discordância, a decisão final será tomada pelo Supervisor da Equipe.

Art. 23. Poderão participar das reuniões da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos pessoas físicas ou jurídicas que possam contribuir com os trabalhos da Equipe, mediante convite do Coordenador.

Subgrupos

Art. 24. É vedada a criação se subgrupos.

Disposições finais e transitórias

Art. 25. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos deverá promover a adequada divulgação dos seus canais de atendimento e, principalmente, aqueles destinados ao registro e comunicação de incidentes cibernéticos na CAPES, informando os horários disponíveis e de eventuais plantões.

Cláusula de revogação

Art. 26. Fica revogada a Portaria GAB/CAPES nº 138, de 2 de outubro de 2013.

Vigência

Art. 27. Esta Portaria entra em vigor em 1º de julho de 2022.

CLAUDIA MANSANI QUEDA DE TOLEDO