ABMES

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 07/10/2024 | Edição: 194 | Seção: 1 | Página: 15
Órgão: Ministério da Educação/Gabinete do Ministro

PORTARIA MEC Nº 989, DE 3 DE OUTUBRO DE 2024

Institui, regulamenta e designa a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério da Educação - Etir-MEC.

O MINISTRO DE ESTADO DA EDUCAÇÃO substituto, no uso das atribuições que lhe confere o art. 87, parágrafo único, inciso II e IV, da Constituição, e tendo em vista o disposto no art. 15, inciso VII, do Decreto nº 9.637, de 26 de dezembro de 2018, resolve:

Art. 1º Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério da Educação - Etir-MEC e regulamentadas suas atribuições e competências, em consonância com a Portaria MEC nº 495, de 18 de julho de 2022, que institui a Política Corporativa de Segurança da Informação e Proteção de Dados - PSI, e com as instruções relacionadas à segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

Art. 2º Para os fins desta Portaria, as definições gerais e todos os termos utilizados neste documento se baseiam no Glossário de Segurança da Informação, publicado pelo Gabinete de Segurança Institucional da Presidência da República e aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO I

DO DOCUMENTO DE CONSTITUIÇÃO

Seção I

Da missão

Art. 3º A Etir-MEC tem como missão planejar, coordenar e executar atividades de prevenção, tratamento e resposta a incidentes cibernéticos, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado ao ambiente digital, à recuperação de sistemas, à análise de ataques e a intrusões, com objetivo de preservar os dados, as informações e a infraestrutura do Ministério da Educação.

Art. 4º A Etir-MEC é responsável por monitorar, receber, analisar e responder às notificações e atividades relacionas a incidentes cibernéticos no âmbito do Ministério da Educação.

Seção II

Da comunidade e do público-alvo

Art. 5º Formam a comunidade ou o público-alvo da Etir-MEC todos os servidores, demais colaboradores e terceiros usuários dos recursos de Tecnologia da Informação e Comunicação - TIC do Ministério da Educação.

Seção III

Do modelo de implementação

Art. 6º A Etir-MEC adotará o modelo de implementação proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, qual seja, Modelo 1 - Utilizando a equipe de Tecnologia da Informação - TI, e será formada por membros das unidades da Subsecretaria de Tecnologia da Informação e Comunicação do Ministério da Educação - STIC/MEC, com experiência e conhecimentos técnicos, que, além de suas funções regulares, desempenharão as atividades relacionadas a prevenção, tratamento e resposta a incidentes cibernéticos.

Seção IV

Da estrutura organizacional

Art. 7º A Etir-MEC poderá ser estendida com a inclusão dos seguintes membros adicionais: representantes legais de áreas específicas do Ministério da Educação, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outros que se entenda adequado, conforme sugerido na Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Art. 8º Para cada membro da Etir-MEC deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades, conforme previsto nas disposições da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Art. 9º A Etir-MEC se relaciona internamente com outras áreas ligadas à Subsecretaria de Tecnologia da Informação e Comunicação. Externamente, a Etir-MEC se relaciona com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, a Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC, o Centro de Segurança Cibernética Integrado do Governo Digital do Brasil - CSIC Gov.br e outras equipes similares da Administração Pública Federal.

Seção V

Da autonomia

Art. 10. A Etir-MEC tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não forem seguidas.

Seção VI

Dos serviços

Art. 11. A Etir-MEC prestará os seguintes serviços:

I - tratamento de incidentes cibernéticos: serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes cibernéticos, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

II - tratamento de artefatos maliciosos: esse serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido, o artefato deverá ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, sua versão e seu objetivo, para

que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa contra esses artefatos;

III - tratamento de vulnerabilidades: esse serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, seu mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

IV - emissão de alertas e advertências: esse serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deverá agir diante do problema;

V - avaliação de segurança: esse serviço tem o objetivo de identificar e avaliar as vulnerabilidades e ameaças existentes nos sistemas e na infraestrutura da instituição. Esse serviço deverá estar alinhado com as melhores práticas e padrões do setor. Esse serviço vai ajudar a garantir que a instituição esteja preparada para enfrentar os desafios de segurança em constante evolução;

VI - detecção de intrusão: o serviço de detecção de intrusão é uma parte essencial de uma equipe de tratamento e resposta a incidentes. Ele tem como objetivo identificar atividades maliciosas, tentativas de comprometimento e intrusões em sistemas e redes da instituição; e

VII - disseminação de informações relacionadas à segurança: o serviço de disseminação de informações relacionadas à segurança é uma parte importante de uma equipe de tratamento e resposta a incidentes. Ele tem como objetivo fornecer informações relevantes sobre segurança da informação para a instituição, seus funcionários e outras partes interessadas, estabelecendo processos de conscientização em incidentes cibernéticos, treinamento para as equipes técnicas envolvidas e a divulgação de incidentes a quem for pertinente.

Parágrafo único. A Subsecretaria de Tecnologia da Informação e Comunicação prestará apoio administrativo aos trabalhos da Etir-MEC.

CAPÍTULO II

DAS RESPONSABILIDADES E COMPETÊNCIAS

Seção I

Do Gestor de Segurança da Informação

Art. 12. Compete ao Gestor de Segurança da Informação no âmbito do tratamento a incidentes cibernéticos:

I - coordenar a instituição, a implementação e a manutenção da infraestrutura necessária para a Etir-MEC, conforme previsto nas disposições das Normas Complementares nº 05/IN01/DSIC/GSIPR e nº 21/IN01/DSIC/GSIPR;

II - garantir que os incidentes cibernéticos nos ambientes digitais do Ministério da Educação sejam monitorados;

III - adotar procedimentos de feedback para assegurar que os servidores, demais colaboradores e terceiros que notificaram incidentes cibernéticos sejam informados dos procedimentos adotados; e

IV - apoiar as atividades rotineiras de conscientização, educação e treinamento em segurança da informação fornecendo casos práticos de incidentes cibernéticos, garantindo-se

a confidencialidade e os devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evitá-los no futuro.

Art. 13. A Etir-MEC está subordinada funcionalmente ao Gestor de Segurança da Informação do Ministério da Educação.

Seção II

Do Agente Responsável

Art. 14. Caberá ao Agente Responsável pela Etir-MEC:

I - estabelecer os procedimentos operacionais e as responsabilidades, gerenciar as atividades e distribuir tarefas para os integrantes da Etir-MEC, inclusive as de caráter proativo;

II - realizar a interlocução com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo;

III - planejar, coordenar e orientar as atividades de monitoramento, recebimento de alertas, análise, classificação e notificação de incidentes cibernéticos;

IV - propor infraestrutura necessária para o funcionamento da Etir-MEC;

V - garantir que os incidentes cibernéticos no ambiente digital do Ministério da Educação sejam registrados e analisados;

VI - informar às autoridades competentes os assuntos relacionados a incidentes cibernéticos;

VII - comunicar de imediato a ocorrência de todos os incidentes cibernéticos ocorridos na sua área de atuação ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, conforme padrão definido por este Órgão;

VIII - interagir com forças policiais especializadas e com o judiciário, nos casos aplicáveis, sobre a ocorrência de incidentes cibernéticos;

IX - informar ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo a ocorrência e as estatísticas de incidentes cibernéticos para manutenção e atualização da base de dados do governo federal;

X - elaborar o Plano de Gestão de Incidentes Cibernéticos;

XI - apresentar, quando solicitado, os resultados das atividades da Etir-MEC ao gestor de segurança da informação do Ministério da Educação;

XII - 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

XIII - acompanhar o processo de identificação e classificação de ativos de informação, o acompanhamento e registro de eventos de segurança e a utilização de metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos quanto ao processo de coleta e preservação de evidências, conforme o disposto na Norma Complementar nº 21/IN01/DSIC/GSIPR.

Parágrafo único. O Agente Responsável pela Etir-MEC deverá ser servidor efetivo de carreira, conforme orientação da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, devendo ser formalmente nomeado, assim como o seu substituto.

Seção III

Da Etir-MEC

Art. 15. A Etir-MEC deverá observar e adotar, no mínimo, os seguintes aspectos e procedimentos, conforme o disposto na Norma Complementar nº 08/IN01/DSIC/GSIPR:

I - registro de incidentes: todos os incidentes cibernéticos notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades da Etir-MEC;

II - tratamento da informação: o tratamento da informação pela Etir-MEC deverá ser realizado de forma a viabilizar e assegurar os princípios de confidencialidade, integridade, disponibilidade e autenticidade da informação, bem como a proteção de dados pessoais e a privacidade, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

III - recursos disponíveis: a Etir-MEC deverá possuir os recursos materiais, tecnológicos e humanos suficientes para prestar os serviços oferecidos para sua comunidade; e

IV - capacitação dos membros: os integrantes da Etir-MEC deverão estar capacitados para operar os recursos disponíveis para a condução dos serviços oferecidos para a sua comunidade.

Art. 16. Ao integrante da Etir-MEC caberá:

I - monitorar, receber, analisar, classificar e responder às notificações e atividades relacionadas a incidentes cibernéticos;

II - armazenar registros para formação de séries históricas como subsídio estatístico e exercer outras atividades que lhe forem acometidas no seu campo de atuação;

III - categorizar, priorizar e atribuir eventos e incidentes cibernéticos;

IV - analisar os impactos, as ameaças ou os danos que ocorreram e qual a reparação e os passos de mitigação que deverão ser seguidos;

V - apoiar no tratamento e na resposta aos incidentes cibernéticos;

VI - recomendar ações para tomada de decisão na recuperação dos incidentes;

VII - efetuar análise e investigação dos incidentes ocorridos no ambiente computacional do Ministério da Educação;

VIII - realizar as atividades de prevenção, de tratamento e de resposta a incidentes cibernéticos na rede computacional do Ministério da Educação;

IX - apoiar a condução de políticas de segurança da informação;

X - priorizar a continuidade dos serviços corporativos na ocorrência de um incidente cibernético;

XI - cumprir o previsto no Plano de Gestão de Incidentes Cibernéticos; e

XII - prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicação.

Art. 17. Os membros integrantes da Etir-MEC deverão ser convocados pelo Agente Responsável pela Equipe, presencialmente ou por videoconferência, com quórum de reunião e de aprovação por maioria simples, para reuniões e deliberações:

I - ordinárias, ao menos uma vez por trimestre, para deliberar sobre a atualização da estratégia de tratamento de incidentes cibernéticos, a ser aprovada por maioria dos membros da Etir-MEC e informada ao Gestor de Segurança da Informação; e

II - extraordinárias, todas as vezes que forem convocados em caso de necessidade de deliberar sobre tomada de decisão para ação de resposta aos incidentes cibernéticos.

CAPÍTULO III

DAS DESIGNAÇÕES

Art. 18. Ficam designados como Agente Responsável, titular e substituto, pela Etir-MEC, os servidores:

I - Alonso Cláudio Pereira da Silva Brito, Matrícula Siape nº 1087782, lotado na Coordenação-Geral de Infraestrutura, Serviços e Segurança da Informação - CGIS/STIC, para atuar como Agente Responsável pela Etir-MEC; e

II - Ulysses da Rocha Rezende, Matrícula Siape nº 3692525, lotado na Coordenação-Geral de Infraestrutura, Serviços e Segurança da Informação - CGIS/STIC, como seu substituto.

Art. 19. Ficam designados como integrantes da Etir-MEC:

I - titular: Coordenador(a)-Geral de Infraestrutura, Serviços e Segurança da Informação (CGIS/STIC);

II - substituto: Coordenador(a) de Infraestrutura e Serviços (CIS/CGIS/STIC);

III - titular: Chefe de Projeto de Infraestrutura e Serviços de Tecnologia (CGIS/STIC);

IV - substituto: Coordenador(a) de Desenvolvimento e Sustentação (CDS/CGSA/STIC);

V - titular: Coordenador(a)-Geral de Dados e Analytics (CGDA/STIC);

VI - substituto: Coordenador(a) de Governança de Dados (CGD/CGDA/STIC);

VII - titular: Coordenador(a)-Geral de Sistemas e Aplicações (CGSA/STIC);

VIII - substituto: Coordenador(a) de Aplicativos e Portais (CAPP/CGSA/STIC);

IX - titular: Chefe de Projeto de Sistemas (DSIS/CAPP/CGSA/STIC);

X - substituto: Chefe de Projeto de Sítios e Portais (CAPP/CGSA/STIC);

XI - titular: Coordenador(a)-Geral de Arquitetura de Tecnologia da Informação (CGATI/STIC); e

XII - substituto: Chefe de Núcleo de Arquitetura (NAR/CASI/CGATI/STIC).

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 20. Esta Portaria deverá ser revisada ao menos uma vez a cada quatro anos, a partir da data da publicação, para que seja adequada às normas e legislações vigentes à época ou sempre que houver necessidade de adequação.

Art. 21. Fica revogada a Portaria MEC nº 4, de 28 de agosto de 2014.

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

LEONARDO OSVALDO BARCHINI ROSA