AGÊNCIA ESPACIAL BRASILEIRA

PORTARIA Nº 795, DE 23 DE MARÇO DE 2022

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais da Agência Espacial Brasileira (ETIR-AEB).

O **PRESIDENTE DA AGÊNCIA ESPACIAL BRASILEIRA**, no uso das atribuições que lhe foram conferidas pela Lei nº 8.854, de 10 de fevereiro de 1994, e pelo Decreto nº 10.469, de 19 de agosto de 2020, e

CONSIDERANDO a Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República - IN/GSI/PR, de 27 de maio de 2020;

CONSIDERANDO a Norma Complementar nº 5/IN01/DSIC/GSIPR, de 17 de agosto 2009;

CONSIDERANDO a Norma Complementar nº 8/IN01/DSIC/GSIPR, de 24 de agosto de 2010;

CONSIDERANDO a Norma Complementar nº 21/IN01/DSIC/GSIPR, de 10 de outubro de 2014;

CONSIDERANDO a Política de Segurança da Informação e Comunicação da AEB vigente;

CONSIDERANDO a Norma Complementar nº 02/POSIC/AEB vigente,

R E S O L V E :

Art. 1º Instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais da Agência Espacial Brasileira (ETIR-AEB).

Parágrafo único. As atividades pertinentes da ETIR-AEB incluem os usuários e serviços de Tecnologia da Informação e Comunicação (TIC) e dos sistemas de informação mantidos na AEB em Brasília, nas Unidades Regionais de Alcântara/MA, Natal/RN e São José dos Campos/SP.

Art. 2º A ETIR-AEB será formada por membros da Coordenação de Tecnologia da Informação e Comunicação da Agência Espacial Brasileira, sendo:

I - Coordenador de Tecnologia da Informação e Comunicação, que coordenará a ETIR e exercerá a função de Gestor de Segurança da Informação Interno, conforme inciso III do art. 2º da Portaria AEB nº 361, de 16 de outubro de 2020;

II - Chefe da Divisão de Projetos e Soluções Corporativas; e

III - Chefe da Divisão de Infraestrutura e Segurança.

Parágrafo único. As funções e serviços de tratamento de incidente serão realizados por administradores de redes, de sistemas e por peritos em segurança, conforme subitem 7.1 da Norma Complementar nº 5/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Art. 3º Para efeito desta Portaria ficam estabelecidos os seguintes termos e definições, em complemento àqueles definidos na Política de Segurança da Informação e Comunicações (POSIC) da Agência Espacial Brasileira:

I - comunidade ou público-alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR;

II - agente responsável da ETIR-AEB: servidor público ocupante de cargo efetivo ou entidade da administração pública federal, direta ou indireta, incumbido de chefiar e gerenciar a ETIR-AEB;

III - CTIR-GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

IV - Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade para agir proativamente com o objetivo de evitar que ocorram incidentes de segurança e receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

V - incidentes de segurança: um evento singular ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

VI - serviço: conjunto de procedimentos estruturados em um processo bem definido, oferecido à comunidade da ETIR-AEB;

VII - 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, possibilitem a identificação de tendências; e

VIII - vulnerabilidades: quaisquer fragilidades dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

Art. 4º A ETIR-AEB possui autonomia completa para tomada de decisões, de acordo com o subitem 9.1 da Norma Complementar nº 5/IN01/DSIC/GSIPR, de 2009, e conduzirá o seu público-alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança.

§ 1º O processo de tomada de decisão sobre o tratamento e medidas adotadas será realizado entre os membros da ETIR-AEB, de modo compartilhado, por maioria simples entre seus membros.

§ 2º Uma vez tomada a decisão, caberá a ETIR-AEB adotar as medidas técnicas necessárias para a recuperação e tratamento do incidente e demais providências técnicas previstas.

§ 3º Durante um incidente de segurança, se devidamente justificada, a equipe poderá tomar a decisão de executar as medidas de recuperação sem esperar pela aprovação de níveis superiores de gestão.

§ 4º As atividades pertinentes a ETIR-AEB serão realizadas com o intercâmbio de informações e em cooperação com as seguintes instâncias:

I - Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Pesquisa (RNP);

II - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV);

III - outras Equipes de Resposta a Tratamento de Incidentes de Segurança da informação da Administração Pública Federal; e

IV - Órgãos, entidades, empresas públicas ou privadas que tenham contratos, acordos ou convênios com a Agência Espacial Brasileira.

§ 5º A ETIR-AEB atuará segundo políticas e procedimentos técnicos e normativos de tratamento de incidentes de rede e poderá se valer de boas práticas de mercado não conflitantes com os dispositivos legais em vigor.

Art. 5º À ETIR-AEB compete:

I - coordenar as atividades de tratamento e resposta a incidentes de segurança na rede de computadores da Agência Espacial Brasileira;

II - definir e documentar a metodologia e os procedimentos internos para o tratamento e resposta a incidentes;

III - criar estratégias de resposta a incidentes de rede previamente conhecidos e executar as ações conforme documentado nos procedimentos;

IV - agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação e Comunicações (SIC) e avaliando condições de segurança de rede por meio de verificações de conformidade;

V - promover a recuperação de serviços e sistemas de Tecnologia da Informação e Comunicações (TIC);

VI - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

VII - receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores da Agência Espacial Brasileira;

VIII - executar as ações necessárias para tratar falhas de segurança;

IX - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

X - cooperar com outras equipes de tratamento e resposta a incidentes;

XI - havendo indícios de ilícitos criminais, informar às autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;

XII - comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, de forma a permitir a geração de estatísticas e soluções integradas;

XIII - sempre que solicitada, apresentar, nas reuniões do Comitê de Segurança da Informação e Comunicações (CSIC/AEB), um resumo dos incidentes de segurança ocorridos na rede de computadores da Agência Espacial Brasileira e as medidas adotadas para solucioná-los; e

XIV - prover o serviço de Tratamento de Incidentes de Segurança e os serviços complementares.

§1º O serviço de Tratamento de Incidentes de Segurança tem por objetivo manter os sistemas e a estrutura de segurança o mais confiável possível, incluindo-se os procedimentos de receber, filtrar, classificar e responder solicitações e alertas.

§ 2º Consideram-se serviços complementares:

I - Tratamento de vulnerabilidades: recebimento de informações sobre vulnerabilidades, em *hardware* ou *software*, analisando a sua natureza e possíveis consequências e desenvolver estratégias para detecção e correção.

II - Emissão de alertas e advertências: divulgação de alertas ou advertências imediatas como uma reação diante de um incidente de segurança, com o objetivo de advertir ou dar orientações sobre como os usuários devem agir diante de um problema.

III - Anúncio: divulgação proativa de alertas sobre vulnerabilidades ou problemas de incidentes de segurança, cujos impactos sejam relevantes, possibilitando que os usuários se preparem para as ameaças em potencial.

Art. 6º Para o desempenho adequado de suas atribuições, os membros da ETIR-AEB deverão ter o patrocínio da alta gestão em capacitações, treinamentos e participação de eventos, *workshops* e congressos nacionais e internacionais em temas relativos a *cybersegurança*, prevenção, tratamento e respostas a incidentes cibernéticos.

Art. 7º Os assuntos de interesse relevante serão levados ao CSIC/AEB visando, principalmente, a prevenção de novos incidentes de segurança.

Art. 8º Casos omissos serão resolvidos pelo Gestor de Segurança da Informação Interno, em observância à Política de Segurança da Informação da Agência Espacial Brasileira e da legislação vigente.

Art. 9º Esta portaria entra em vigor na data da sua publicação.

CARLOS AUGUSTO TEIXEIRA DE MOURA

Presidente da Agência Espacial Brasileira

Documento assinado eletronicamente por **Carlos Augusto Teixeira de Moura**, **Presidente**, em 23/03/2022, às 16:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.aeb.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0149407** e o código CRC **E4E8B100**.

Referência: Processo nº 01350.001766/2021-37 SEI nº 0149407