Boletim de Serviço Eletrônico em 24/10/2023
DOU de 19/10/2023, Seção 1, Página 18

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PORTARIA REI/IFTO Nº 81, DE 02 DE OUTUBRO DE 2023

Institui e regulamenta o trabalho da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins.

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS, reconduzido pelo Decreto Presidencial de 9 de maio de 2022, publicado no Diário Oficial da União de 10 de maio de 2022, seção 2, no uso de suas atribuições legais e regimentais, e considerando a necessidade de garantir a segurança da informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, resolve:

Art. 1º Esta Portaria institui e regulamenta o trabalho da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO), de caráter permanente e de natureza consultiva, visando à deliberação sobre os assuntos relativos a prevenção, tratamento e resposta a incidentes cibernéticos, gestão do processo de continuidade de negócios, elaboração e manutenção de planos, programas e procedimentos sobre segurança da informação, conforme determina a legislação vigente.

Art. 2º A ETIR tem por escopo de atuação a prevenção da ocorrência de incidentes de segurança da informação, a mitigação de riscos relacionados à segurança da informação e a realização de ações reativas que incluem, mas não se limitam a:

I - receber, analisar e responder às notificações e às atividades relacionadas a incidentes de segurança em redes de computadores;

II - desenvolver as atividades de prevenção, tratamento e resposta a incidentes de segurança da informação;

III - notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) sobre a ocorrência de qualquer incidente de segurança, seguindo os formatos e procedimentos estabelecidos pelo CTIR Gov; e

IV - trocar informações acerca de segurança da informação com as demais Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos existentes, seguindo os formatos e procedimentos estabelecidos pelo CTIR Gov.

Art. 3º A ETIR atenderá os usuários da Rede IFTO por chamado registrado eletronicamente na Central de Serviços (Sistema Unificado de Administração Pública —SUAP) ou por mensagem encaminhada para o endereço eletrônico dti@ifto.edu.br.

Art. 4º O IFTO adotará o Modelo 1 apresentado no subitem

7.1 da Norma Complementar 05/IN01/DSIC/GSI/PŔ, de 14 de agosto de 2009.

§ 1º Neste modelo não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de Rede; a ETIR será formada a partir dos membros das equipes de Tecnologia da Informação (TI) do IFTO que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

§ 2º Neste modelo, as funções e os serviços de tratamento de incidentes deverão ser realizados, preferencialmente, por administradores de rede, de suporte ou de sistema ou, ainda, por peritos em segurança.

Art. 5º Para a resolução de incidentes, a ETIR terá dois tipos de autonomia:

I - autonomia completa: para incidentes classificados como incidentes de segurança não críticos, durante o qual a ETIR poderá executar o que julgar necessário e adequado sem esperar pela aprovação de níveis superiores de gestão; e

II - autonomia compartilhada: para incidentes considerados críticos, em que a ETIR poderá recomendar as ações a serem seguidas e deverá indicar suas repercussões caso não sejam seguidas.

Parágrafo único. Na autonomia compartilhada, a ETIR participará do resultado da decisão, sendo apenas um membro no processo decisório; contudo, de forma a reduzir os potenciais impactos dos incidentes, a ETIR terá autonomia para executar medidas de mitigação no ambiente computacional, reportando posteriormente ao grupo decisório as ações implementadas e seus resultados.

Art. 6º A ETIR será composta pelos seguintes representantes do Instituto Federal do Tocantins:

I - Responsável pela Diretoria de Tecnologia da Informação;

II - Representante(s) da Coordenação de Redes e Segurança da Informação;

III - Representante(s) da Coordenação de Governança de TI;

IV - Representante(s) da Coordenação de Sistemas de Informação;

V - Representante(s) da Coordenação de Manutenção e Suporte; e

VI - Gestor de Segurança da Informação.

Art. 7º As unidades organizacionais do IFTO terão a responsabilidade de informar imediatamente à Diretoria de Tecnologia da Informação todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes na rede de computadores, sobre os quais venham a tomar conhecimento.

Art. 8º A ETIR 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 vulnerabilidades: serviço que consiste em analisar possíveis vulnerabilidades, quer sejam em **hardware**, quer sejam em **software**, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção;

III - emissão de alertas, advertências e anúncios: serviço que

consiste em acompanhar alertas ou recomendações emitidas pelo CTIR Gov como medida proativa ou preventiva, com o objetivo de tomar as devidas ações técnicas de tratamento ou mitigação dos respectivos riscos, advertir o público-alvo ou orientá-los sobre as devidas ações;

IV - resolução de incidentes: a ETIR deverá buscar sanar, com prioridade e/ou urgência, os incidentes e as vulnerabilidades cibernéticas detectadas, em especial aquelas identificadas nos alertas e nas recomendações expedidas pelo CTIR GOV, ou que impactem os serviços críticos definidos pelo IFTO;

V - 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, o qual, uma vez recebido, 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; e

VI - elaboração de normas internas: propor diretrizes, procedimentos, medidas e controles que visem à melhoria da segurança da informação.

Art. 9º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação do Instituto Federal do Tocantins, apoiado pelo Comitê Gestor de Tecnologia da Informação, quando necessário.

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

ANTONIO DA LUZ JÚNIOR

Reitor do Instituto Federal do Tocantins

Documento assinado eletronicamente por **Antonio da Luz Júnior**, **Reitor**, em 18/10/2023, às 15:02, 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.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2142668** e o código CRC **7DD8000D**.
