



UNIVERSIDADE FEDERAL DO OESTE DA BAHIA – UFOB

Pró-Reitoria de Tecnologia da Informação e Comunicação - PROTIC

PORTARIA PROTIC/UFOB Nº 02, DE 25 DE JULHO DE 2024

Regulamenta o trabalho da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) da Universidade Federal do Oeste da Bahia (UFOB), de caráter permanente, visando à coordenação no tratamento e resposta a incidentes cibernéticos, gestão do processo de continuidade de negócios, na elaboração e manutenção de planos, conforme determina a legislação vigente.

O PRÓ-REITOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, nomeado pela portaria UFOB Nº 282, de 17 de outubro de 2023, publicada em 18 de outubro de 2023 no Diário Oficial da União, edição 198, seção 2, página 23, no uso das atribuições que lhe confere,

CONSIDERANDO a PORTARIA Nº 38, DE 14 DE AGOSTO DE 2009, DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, que homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR que disciplina a criação das ETIR nos órgãos e entidades da Administração Pública Federal; e

CONSIDERANDO a RESOLUÇÃO CGAG/CONSUNI/UFOB Nº 018, DE 24 DE AGOSTO DE 2023, que institui a Política de Segurança da Informação na UFOB, resolve:

Art. 1º. A ETIR da Universidade Federal do Oeste da Bahia tem por missão planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, podendo receber e notificar eventos que venham a comprometer a segurança da informação de ativos de informação de abrangência da universidade.

Parágrafo Único. As competências da ETIR devem estar alinhadas com a Resolução CGAG/CONSUNI/UFOB Nº 018, de 24 de agosto de 2023.

Art. 2º. A ETIR atende aos domínios e endereços de Protocolo de Internet (IPs) sob responsabilidade da Universidade Federal do Oeste da Bahia, e membros da comunidade acadêmica que estejam sob a utilização da rede institucional ou serviços tecnológicos da instituição.

Art. 3º. A Universidade Federal do Oeste da Bahia adotará o modelo de implementação nº 1 que trata da utilização da Equipe de Tecnologia da Informação conforme a Norma Complementar 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009.

Parágrafo Único. 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 do Órgão responsável pela Tecnologia da Informação e Comunicação da Universidade conforme portaria vigente.

Art. 4º A ETIR possuirá autonomia compartilhada nos processos decisórios referentes às ações de prevenção e ações a serem tomadas para conter incidentes de segurança cibernética, nos termos do Capítulo 9 da Norma Complementar no 05/IN01/DSIC/GSIPR.

§ 1º Os membros do processo decisórios serão compostos pelo:

I - gestor de segurança da informação, que coordena a ETIR;

II - responsável do órgão de Tecnologia da Informação e Comunicação (TIC); e

III - responsáveis pelas coordenadorias vinculadas ao órgão de TIC.

§ 2º Após definir a decisão, a ETIR deve adotar as medidas técnicas necessárias para a recuperação e tratamento do incidente.

§ 3º A ETIR atuará de forma sinérgica com as demais áreas, unidades organizacionais ou órgãos colegiados de TIC..

§ 4º Os gestores das áreas de TIC devem auxiliar e cooperar com a ETIR na ocorrência de crises oriundas de incidentes cibernéticos.

Art. 5º. Os serviços prestados pela ETIR serão dados inicialmente por:

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, com o objetivo de 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 Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - 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;

§ 1º A descrição das ações relativas aos serviços dos incisos I e II farão parte do plano de contingência frente à incidentes.

§ 2º O serviço ao que se refere o inciso III poderá ser utilizado através de canais oficiais de comunicação da própria ETIR e adotados pela universidade tais como: e-mail institucional, publicações em páginas ou plataformas de comunicação da universidade.

§ 3º A formalização que tratam os incisos I, II e III farão parte do Processo de Tratamento e Resposta a Incidentes a ser construído pela própria ETIR.

§ 4º Os serviços elencados não comprometem a inclusão de outras atividades necessárias à segurança da informação observando a legislação vigente.

Art. 6º. Esta Portaria entra em vigor na data de sua publicação.

Uiliam Rangel Amorim Souza
Pró-reitor de Tecnologia da Informação e Comunicação