SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
GAB - GABINETE DO REITOR

PORTARIA GAB/FURG N° 48, DE 07 DE JULHO DE 2023

Dispõe sobre a a criação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), no âmbito da Universidade Federal do Rio Grande - FURG.

O REITOR DA UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG, no uso das atribuições que lhe conferem o Estatuto e o Regimento Geral da Universidade e considerando:

a. o Decreto nº 9.637, de 26 de dezembro de 2018;

b. o Decreto nº 10.748, de 26 de julho de 2021;

c. a Resolução CONSUN/FURG nº 5, de 20 de maio de 2022, que dispõe sobre a Política de Segurança da Informação (PSI/FURG) da FURG;

d. a Instrução Normativa nº 1, de 27 de maio de 2020, da Presidência da República;

e. a Norma Complementar nº 5/IN01/DSIC/GSIPR;

f. a Norma Complementar nº 8/IN01/DSIC/GSIPR;

g. a Norma Complementar nº 20/IN01/DSIC/GSIPR; e

h. a Norma Complementar nº 21/IN01/DSIC/GSIPR,

RESOLVE:

Art. 1º Instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/FURG), no âmbito da Universidade Federal do Rio Grande - FURG, subordinada ao Comitê Gestor de Segurança da Informação (CGSI), a fim de promover as ações necessárias ao cumprimento da legislação vigente, observando, também, as diretrizes estabelecidas na Política de Segurança da Informação (PSI) da instituição.

Parágrafo único. Integram o presente documento normas gerais e específicas do gerenciamento de incidentes cibernéticos, bem como os conceitos do Anexo I.

Art. 2º A ETIR/FURG tem como missão coordenar as atividades de tratamento e resposta a incidentes cibernéticos, monitorar as redes, seus serviços e suas vulnerabilidades, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, preservando, assim, os dados, as informações e a infraestrutura de rede da FURG.

Parágrafo único. A ETIR/FURG atenderá diretamente todas as unidades da FURG, seus usuários e solicitantes externos que registrarem eventos identificados como incidentes cibernéticos.

Art. 3º A ETIR/FURG será constituída pelo agente responsável, por titulares, suplentes e equipe de apoio (membros convidados), de diversas áreas, atribuindo um caráter multidisciplinar para a A ETIR/FURG.

Art. 4º A ETIR/FURG será estabelecida conforme a Norma Complementar Nº 05/IN01/DSIC/GSICPR, Modelo 1 - Utilizando a equipe de Tecnologia da Informação (TI) existente, onde:

I- o Chefe da Divisão de Segurança da Informação do Centro de Gestão de Tecnologia da Informação (DSI/CGTI) será designado como Agente Responsável pela ETIR;

II- o Agente Responsável, extraordinariamente, poderá convocar representantes de outros setores do CGTI ou outras unidades/setores da FURG para atuarem na Equipe de Apoio para o tratamento e resposta de determinado incidente cibernético;

III- a DSI/CGTI deverá atuar como Equipe Central coordenando e atuando as atividades da ETIR/FURG; e

IV- a Equipe de Apoio será composta por servidores membros convidados de outros setores da Universidade.

Art. 5º A ETIR seguirá o Modelo “Autonomia Compartilhada”, conforme a Norma Complementar Nº 05/IN01/DSIC/GSICPR, detalhado no Plano de Gestão de Incidentes Cibernéticos da FURG.

Art. 6° A ETIR/FURG desempenhará os seguintes serviços:

I- tratamento de vulnerabilidades;

II- tratamento de incidentes cibernéticos;

III- emissão de alertas e advertências;

IV- anúncios e disseminação de informações relacionadas à segurança; .

V- detecção de intrusão; e

VI- outras atividades determinadas pelo CGSI.

Parágrafo único: conforme a necessidade da ETIR/FURG, outros serviços poderão ser oferecidos.

Art. 7° À ETIR/FURG compete:

I- garantir que os incidentes cibernéticos na FURG sejam monitorados;

II- desenvolver e implantar o Plano de Gestão de Incidentes Cibernéticos e o Plano de Comunicação de Incidentes Cibernéticos;

III- executar a emissão de alertas e advertências relacionadas a vulnerabilidades e incidentes cibernéticos;

IV- disseminar informações relacionadas à segurança, que sejam ostensivas, e que facilitem a pesquisa e utilização;

V- executar as atividades de tratamento e resposta a incidentes cibernéticos, enviando alertas aos responsáveis e cobrando o retorno em tempo hábil;

VI- executar, quando possível, o tratamento de artefatos maliciosos e vulnerabilidades;

VII- efetuar a análise de segurança na infraestrutura de redes e serviços computacionais da FURG com base nas necessidades e nas melhores práticas de mercado;

VIII- observar os procedimentos de forense digital para registro de eventos, coleta e preservação de evidências de incidentes cibernéticos;

IX- apoiar tecnicamente na elaboração de políticas, normas, notas técnicas e procedimentos direcionados a segurança da informação da FURG; e

X- apoiar, quando demandada, no acionamento de autoridades policiais competentes para a adoção dos procedimentos legais.

Art. 8° Ao Agente Responsável pela ETIR/FURG compete:

I- coordenar o processo de comunicação entre a ETIR/FURG e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov), conforme legislação vigente;

II- coordenar as atividades da ETIR/FURG;

III- propor ajustes e medidas preventivas e preditivas ao CGSI/FURG referentes a incidentes ou vulnerabilidades na rede da FURG; e

IV- apoiar e buscar os meios necessários para capacitação dos membros da ETIR/FURG relacionada à segurança da informação.

Art. 9° A comunicação de incidentes cibernéticos na rede FURG deve ser feita através dos seguintes canais:

I- solicitantes internos:

a) canal de “Solicitações” do Sistemas FURG;

b) e-mail: etir@furg.br;

c) telefone: (53) 3233-6568; e

d. presencialmente no CGTI, em casos emergenciais.

II- solicitantes externos:

a) e-mail: etir@furg.br;

b) telefone: (53) 3233-6568; e

c) correspondências oficiais (memorandos, ofícios).

Art. 10. Os casos omissos serão resolvidos pelo CGSI, que poderá adotar o que julgar mais adequado, observadas as disposições desta normativa e a legislação pertinente.

Art. 11. Esta Portaria poderá ser revisada periodicamente, quando necessário.

Art. 12. O disposto nesta Portaria entra em vigor na data de sua publicação, revogando orientações em contrário.

Danilo Giroldo

Reitor

Documento assinado eletronicamente por **Danilo Giroldo**, **Reitor**, em 11/07/2023, às 17:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.furg.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0 informando o código verificador **0082943** e o código CRC **8D57C997**.

ANEXO N° I, DE 10 DE JULHO DE 2023

ANEXO I – DOS CONCEITOS

(PORTARIA GAB/FURG N° 48, DE 7 DE JULHO DE 2023)

Agente responsável: servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Autonomia: descreve o escopo de atuação e o nível de responsabilidade que a ETIR tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores. A autonomia define o nível de controle da ETIR no relacionamento com os componentes da sua organização.

Autonomia compartilhada: os níveis de autonomia serão dependentes do tipo de incidente, de acordo com a sua criticidade, e serão definidos no Plano de Tratamento de Incidentes Cibernéticos.

Detecção de intrusão: consiste no monitoramento e análise da rede e servidores, através de softwares dedicados a essa função com vistas a identificar e iniciar os procedimentos de resposta a incidentes cibernéticos.

Emissão de alertas e advertências: consiste em divulgar alertas ou advertências imediatas, como uma reação, diante de um incidente de segurança ocorrido em redes de computadores, com o objetivo de dar orientações sobre como a comunidade deve agir diante do problema.

Emissão de anúncios e disseminação de informações relacionadas à segurança: consiste em divulgar, de forma preventiva, anúncios sobre vulnerabilidades e problemas de incidentes de segurança possibilitando que a comunidade se prepare contra possíveis ameaças.

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética da FURG em observância à Política de Segurança da Informação (PSI).

Incidente cibernético: ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade, conformidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema.

Plano de Gestão de Incidentes Cibernéticos: plano que orienta as equipes sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos.

Plano de Comunicação de Incidentes Cibernéticos: parte integrante do Plano de Gestão de Incidentes Cibernéticos que descreve especificamente as diretrizes e procedimentos para a comunicação de informações relacionadas a incidentes cibernéticos entre as partes interessadas.

Segurança da informação: diretrizes, objetivos e estruturas voltadas à proteção da informação contra ameaças pautadas nos princípios de confidencialidade, integridade, disponibilidade, autenticidade e conformidade, conforme a Política de Segurança da Informação da FURG (PSI-FURG).

Solicitante interno: servidor, aluno ou colaborador da FURG credenciado que tenha acesso aos Sistemas FURG.

Solicitante externo: pessoa física ou jurídica, que não seja caracterizada como solicitante interno.

Tratamento de incidentes cibernéticos: consiste em receber, filtrar, classificar, tratar, 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.

Tratamento de vulnerabilidades: consiste em receber informações sobre vulnerabilidades, objetivando analisar sua natureza, mecanismo, suas consequências e desenvolver estratégias para detecção e correção.

Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.