MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA
REITORIA
Conselho Superior
Rua Fernão Dias Paes Leme, 11, Calungá, Boa Vista - RR, CEP 69303220 ,
www.ifrr.edu.br

Resolução CONSUP/IFRR N° 809, de 25 de novembro de 2024.

Institui o Regimento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética do Instituto Federal de Educação, Ciência e Tecnologia de Roraima - IFRR

A presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, no uso de suas atribuições legais, tendo em vista o que consta no Processo nº 23231.000434.2024-77 - Elaboração do Regimento da ETIR, e a decisão do colegiado tomada na 94ª sessão plenária, realizada em 11 de outubro de 2024,

RESOLVE:

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução dispõe sobre o regimento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Instituto Federal de Educação, Ciência e Tecnologia de Roraima (IFRR), foi elaborado por Comissão instituída pela Portaria Nº 0683/GAB-REITORIA/IFRR, de 28 de fevereiro 2024 com o objetivo de atender ao Art. 18 da Política de Segurança da Informação e Comunicação (POSIC), disposta pela Resolução 790/2024.

Art. 2º Para os fins deste regimento devem ser adotadas as seguintes definições:

I. ETIR: equipe de pessoas com a responsabilidade por receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores e sistemas de informação;

II. Centro de prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR GOV): Subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI;

III. agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar uma ETIR;

IV. artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V. comunidade ou público alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI. comunidade acadêmica: conjunto de pessoas composto por estudantes, professores,

pesquisadores, técnicos administrativos e prestadores de serviço.

VII. incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VIII. serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

IX. tratamento de incidentes de segurança em redes computacionais: 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;

X. usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do IFRR, independentemente do vínculo com o IFRR (alunos, contratados, consultores, conselheiros, servidores, temporários, sociedade em geral e etc.); e

XI. vulnerabilidade: qualquer fragilidade dos sistemas de informação e redes de computadores que permitam a exploração maliciosa e acessos indesejados ou não autorizados.

CAPÍTULO II - MISSÃO

Art. 3º A ETIR-IFRR tem como missão prioritária a facilitação e a coordenação das atividades de atendimento às demandas internas da instituição em consonância com as atividades de resposta e tratamento a incidentes em redes de computadores.

CAPÍTULO III - COMUNIDADE

Art. 4º O público alvo da ETIR é o domínio .ifrr.edu.br, endereços IP alocados ao IFRR e a usuários da comunidade acadêmica.

Art. 5º A ETIR irá se relacionar com os demais organismos de tratamentos de incidentes, nas seguintes condições:

I. A ETIR-IFRR deve colaborar com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR-Gov), que é responsável por coordenar a resposta a incidentes cibernéticos em âmbito governamental;

II. As ETIR's ou equipes técnicas equivalente de empresas prestadoras de serviços de tecnologia contratadas pelo IFRR;

III. As ETIR's ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o IFRR;

IV. O Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) para alinhar estratégias de segurança da informação em nível nacional.

CAPÍTULO IV - MODELO DE IMPLEMENTAÇÃO

Art. 6º A implementação e o funcionamento da ETIR seguirão este regimento, criado com base na metodologia definida pelo GSI/PR na Norma Complementar 05/IN01/DSIC/GSIPR, contendo as seguintes diretrizes:

I. utilizará a equipe de Tecnologia da Informação (TI): não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de segurança cibernética. A Equipe será formada a partir dos membros das equipes de TI do próprio IFRR, que além de suas funções regulares passarão a desempenhar as atividades dispostas nos Artº 13;

II. neste modelo as funções e serviços de tratamento e resposta de incidentes deverão ser realizados, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos ou especialista de segurança;

III. a ETIR-IFRR desempenhará suas atividades, via de regra, de forma reativa, sendo recomendável, porém, que oAgente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades preventivas;

CAPÍTULO V - ESTRUTURA ORGANIZACIONAL

Art 7º Cabe ao Gestor de Segurança da Informação, que também é presidente do Comitê Gestor de Segurança da Informação (CGSI) a responsabilidade de coordenação, implementação e manutenção da infraestrutura necessária à ETIR-IFRR, conforme item VIII do Art. 6º, Seção III do regimento do CGSI do IFRR, instituído pela Resolução 685/2022.

Parágrafo único. O CGSI também é responsável por definir, junto à área de gestão de pessoas do IFRR e à própria ETIR, as necessidades de capacitação e o aperfeiçoamento técnico dos membros da ETIR.

Art 8º Com relação ao organograma institucional, a ETIR ficará vinculada à Diretoria de Tecnologia da Informação - DTI da reitoria do IFRR.

Art. 9º Os membros da ETIR, devem ser indicados pelo CGSI e nomeados por meio de portaria emitida pelo(a) reitor(a), e esta deverá ser atualizada sempre que houver alteração de algum dos membros.

Art 10º O responsável pelo Núcleo de Infraestrutura e Redes (NIR) será o Agente Responsável pela ETIR.

Parágrafo único. Em caso de licença, afastamento ou férias do Agente Responsável, este deverá designar como seu substituto um Membro da Equipe.

Art 11º Compete ao Agente Responsável pela ETIR:

I. planejar, coordenar e orientar as atividades de monitoramento, recebimento de alertas, análise, classificação e notificação de incidentes de segurança;

II. propor a implementação da infraestrutura necessária para o funcionamento da ETIR;

III. propor as providências necessárias para a capacitação e o aperfeiçoamento técnico dos membros da ETIR;

IV. garantir que os incidentes de segurança cibernética do IFRR sejam registrados e analisados;

V. informar às autoridades competentes os assuntos relacionados a incidentes de segurança cibernética;

VI. articular, juntamente com o Diretor da DTI, quando necessário, com autoridades policiais e judiciárias, outros CTIR e outras ETIR, para troca de informações e experiências, com o objetivo de antecipar tendências ou padrões de ataques em massa;

VII. informar ao Centro de Tratamento de Incidentes de Redes do Governo - CTIR Gov a ocorrência e as estatísticas de incidentes de segurança, para manutenção e atualização da base de dados do governo federal;

VIII. disseminar, no âmbito do IFRR, alertas de vulnerabilidades, informativos sobre novas atualizações e incidentes de segurança tratados ou qualquer assunto relacionado à segurança da rede de computadores ou sistemas de informação; e

IX. propor a adoção e padronização de técnicas, soluções e demais medidas que envolvem a Segurança em Redes Computacionais no âmbito do IFRR. As proposições deverão ser discutidas juntamente com o Gestor de Segurança da Informação e com o Diretor de Tecnologia da Informação.

Art. 12º Os membros permanentes da ETIR devem estar vinculados à Reitoria, um número mínimo de 5 (cinco) membros da Diretoria de Tecnologia da Informação (DTI), distribuídos da seguintes forma:

I. todos os servidores lotados na NIR;

II. 2(dois) servidores do suporte ao usuário e

III. 2 (dois) servidores oriundos da Coordenação de Desenvolvimento e Suporte a Sistemas (CDSS).

Art. 13º Compete aos membros permanentes da ETIR:

I. monitorar, receber e registrar eventos, elaborar relatórios de incidentes de segurança e alertas;

II. categorizar, priorizar e atribuir eventos e incidentes de segurança;

III. analisar os incidentes de segurança procurando extrair informações que permitam impedir a continuidade da ação maliciosa e os impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos;

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

V. reunir-se com periodicidade mínima equivalente aos relatórios de planejamento de trabalho institucional, podendo realizar mais reuniões de acordo com as demandas.

Art. 14º Cada unidade de ensino do IFRR deverá possuir ao menos um membro colaborador na ETIR.

Parágrafo único. Para cada membro colaborador da ETIR deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades.

Art. 15º Compete aos membros colaboradores da ETIR:

I. iniciar o tratamento de quaisquer incidentes de segurança em redes de computadores ocorridos em sua unidade e relatá-los imediatamente ao Agente Responsável pela ETIR para realização das medidas necessárias;

II. ele passa a colaborar com a ETIR nos incidentes reportados em suas respectivas unidades;

III. atuar em caso de necessidade de expertise em ocorrências que extrapolam suas unidades de origem, conforme interesse do Agente Responsável pela ETIR.

CAPÍTULO VI - DA AUTONOMIA

Art. 16º A ETIR terá autonomia compartilhada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do IFRR somente com anuência do Diretor de Tecnologia da Informação e Unidade Gestora responsável pela área/sistema afetada, e deverá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

§1º A ETIR deverá participar do processo de tomada de decisão sobre quais medidas de combate e prevenção deverão ser adotadas para os incidentes de segurança cibernética.

§2º A ETIR poderá recomendar e/ou realizar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com o Gestor de Segurança da Informação e com o Diretor de Tecnologia da Informação.

CAPÍTULO VII - SERVIÇO

Art. 17º A ETIR fornecerá o serviço de Prevenção e Tratamento de Incidentes de Segurança em Redes Computacionais e Sistemas de Informação, que compreende as seguintes ações:

I. recepção de solicitações e alertas diversos, utilizando como canal de comunicação a central de serviços do SUAP e o e-mail etir@ifrr.edu.br;

II. filtragem de todo conteúdo direcionado à ETIR, para fins de verificação quanto à necessidade

de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais ou sistemas de informação, encaminhar para a área competente;

III. catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV. classificação dos incidentes detectados quanto ao nível de severidade e impacto, sendo: muito baixo, baixo, médio, grave, muito grave;

V. tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI. recolhimento de provas o quanto antes após a ocorrência de um incidente de segurança da Informação;

VII. execução de análise sobre os registros de falha para assegurar que estas foram satisfatoriamente atendidas;

VIII. submissão ao Gestor de Segurança da Informação e ao Diretor de Tecnologia da Informação dos procedimentos adotados e as ocorrências de violação às normas de segurança da informação do IFRR;

IX. Indicar a necessidade de controles para limitar a frequência e os danos de futuras ocorrências de incidentes de segurança em redes de computadores e sistemas de informação;

X. emitir relatório anual ou sob-requisição do Gestor de Segurança da Informação contendo o resumo das ocorrências de incidentes de segurança para apresentação ao CGSI/CGD;

XI. notificar o Gestor de Segurança da Informação a respeito dos eventos e incidentes de segurança da informação na rede de computadores do IFRR que ensejem aplicação de penalidades previstas na Política de Segurança da Informação (PSI) vigente do IFRR;

XII. responder às solicitações e alertas encaminhados para a ETIR-IFRR;

XIII. monitoramento da aplicação do tratamento dos incidentes indicados; e

XIV. elaborar Matriz GUT para as atividades que envolvem a segurança da informação (Gravidade, Urgência e Tendência) para o devido planejamento, priorização e tratamento das vulnerabilidades identificadas nas redes de computadores ou sistemas de informação do IFRR.

Art. 18º O detalhamento dos demais serviços prestados pela ETIR-IFRR deverá ser elaborado pela equipe, obedecendo aos critérios estabelecidos da Norma Complementar 05/IN01/DSIC/GSIPR, posteriormente encaminhado à DTI e ao Gestor de Segurança da Informação.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 19º A ETIR-IFRR deve fomentar ações de conscientização para que os servidores, colaboradores e demais usuários de sistemas de Tecnologia de Informação do IFRR comuniquem à ETIR-IFRR, o mais breve possível, toda e qualquer falha, anomalia, ameaça ou vulnerabilidade identificada, mesmo que seja apenas uma suspeita.

Art. 20º A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo CTIR GOV e demais legislações federais sobre segurança da informação.

Art. 21º A ETIR poderá usar as melhores práticas e soluções de mercado, desde que não conflitem com os dispositivos desta Norma Complementar ou Normas Internas do IFRR.

Art. 22º A troca de informações e a forma de comunicação entre a ETIR-IFRR e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

Art. 23º Os casos omissos ou não regulamentados nesta norma serão tratados pelo Comitê

Gestor de Segurança da Informação (CGSI) do IFRR.

Art. 24º Esta norma entra em vigor na data da sua publicação.

Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, em Boa Vista-RR, 8 de novembro de 2024.

Aline Cavalcante Ferreira
Presidente em exercício do CONSUP

Documento assinado eletronicamente por:

- **Aline Cavalcante Ferreira**, **REITOR(A) - SUB-CHEFIA - GAB**, em 25/11/2024 09:05:56.

Este documento foi emitido pelo SUAP em 07/11/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrr.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 312556
Código de Autenticação: c34063f31c