Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS
Avenida Vicente Simões, 1.111, Nova Pouso Alegre, POUSO ALEGRE / MG, CEP 37553-465 - Fone: (35) 3449-6150

RESOLUCAO Nº196/2022/CONSUP/IFSULDEMINAS

18 de maio de 2022

Dispõe sobre a aprovação do Regimento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-IFSULDEMINAS.

O Reitor e Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais, Professor Marcelo Bregagnoli, nomeado pelo Decreto de 23 de julho de 2018, DOU nº 141/2018 – seção 2, página 1 e em conformidade com a Lei 11.892/2008, no uso de suas atribuições legais e regimentais, em reunião realizada em dezoito de maio de 2022, **RESOLVE:**

Art. 1º - Considerando:

1. A Resolução Nº 066/2020, de 15 de dezembro de 2020, que dispõe sobre a aprovação da Política de Governança de Tecnologia da Informação (PGTI) do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais - IFSULDEMINAS; e

2. A Resolução Nº 050/2016, de 28 de junho de 2016, que dispõe sobre a Política de Segurança da Informação (PSI) e sobre o Sistema de Gestão de Segurança da Informação (SGSI) do IFSULDEMINAS; e

3. A Portaria Nº 1970/2019 - GAB/RET/IFSULDEMINAS, que institui a Política de Gestão de Riscos de TI do IFSULDEMINAS; e

4. O Decreto Nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos; e

5. A Norma Complementar nº 05/IN01/DSIC/GSIPR, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal; e

6. A Norma Complementar nº 08/IN01/DSIC/GSIPR, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

Art. 2º - **Aprovar** o Regimento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-IFSULDEMINAS.

Art. 3º - Esta Resolução entra em vigor na data de sua assinatura.

Marcelo Bregagnoli
Presidente do Conselho Superior
IFSULDEMINAS

REGIMENTO DA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-IFSULDEMINAS

CAPÍTULO I - OBJETIVO

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-IFSULDEMINAS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do IFSULDEMINAS.

Art. 2º As atividades pertinentes à ETIR-IFSULDEMINAS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do IFSULDEMINAS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - as ETIRs ou equipe técnica equivalente de empresas prestadoras de serviços de tecnologia contratadas pelo IFSULDEMINAS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o IFSULDEMINAS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - GSI/PR.

CAPÍTULO II - DEFINIÇÕES

Art. 3º Para os efeitos desta Resolução fica estabelecida a seguinte terminologia:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores e sistemas de informação;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, 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 ou militar de carreira 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 - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

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

VIII - 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;

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

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou para uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III - MODELO DE IMPLEMENTAÇÃO

Art. 4º A implementação e o funcionamento da ETIR-IFSULDEMINAS seguirão este regimento, criado com base na metodologia definida pelo GSI/PR, contendo as seguintes diretrizes:

I - basear-se no "Modelo 1 - Utilizando a equipe de Tecnologia da Informação", conforme proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação – DTI do IFSULDEMINAS e nos NTIs dos campi, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-IFSULDEMINAS;

III – a ETIR-IFSULDEMINAS desempenhará suas atividades, via de regra, de forma reativa, sendo recomendável, porém, que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades proativas;

IVI - a ETIR-IFSULDEMINAS ficará vinculada tecnicamente à Diretoria de Tecnologia da Informação - DTI da reitoria do IFSULDEMINAS;

V - o Coordenador de Infraestrutura de Tecnologia da Informação – CITI-DTI será o Agente Responsável pela ETIR-IFSULDEMINAS; e

VI - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Diretor da DTI, ou ainda, por algum servidor indicado pelo mesmo (desde que se enquadre no item ii deste artigo).

CAPÍTULO IV - COMPOSIÇÃO

Art. 5º A ETIR-IFSULDEMINAS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores dos campi do IFSULDEMINAS sob supervisão da DTI.

§ 1º Os membros da ETIR-IFSULDEMINAS serão indicados pelo Diretor de Tecnologia da Informação e Coordenadores dos NTIs, e designados por meio de portaria emitida pelo reitor do IFSULDEMINAS;

§ 2º A distribuição dos membros da ETIR-IFSULDEMINAS se dará da seguinte forma:

I - Todos os servidores lotados na Coordenadoria de Infraestrutura de Tecnologia da Informação - CITI-DTI atuarão como membros permanentes;

II - 2 (dois) servidores permanentes, oriundos da Coordenadoria de Suporte de Tecnologia da Informação - CSTI-DTI;

III - 2 (dois) servidores permanentes, oriundos da Coordenadoria de Desenvolvimento de Tecnologia da Informação - CDTI-DTI; e

IV - 1 (um) servidor colaborador, oriundo de cada um dos NTIs dos campi do IFSULDEMINAS, com formação técnica compatível.

Art. 6º Cada unidade do IFSULDEMINAS deverá possuir ao menos um Membro de Equipe na ETIR. Este será responsável por iniciar o tratamento de quaisquer incidentes de segurança em redes de computadores ocorrido em sua unidade e relatá-los imediatamente ao ETIR-IFSULDEMINAS para realização das medidas necessárias.

I. Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR-IFSULDEMINAS.

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

lll. O Comitê de Segurança da Informação da organização (CSI) será o responsável por definir, junto à área de gestão de pessoas do IFSULDEMINAS e à própria ETIR-IFSULDEMINAS, as necessidades de capacitação e o aperfeiçoamento técnico dos membros da ETIR-IFSULDEMINAS.

Art. 7º A equipe ETIR-IFSULDEMINAS, nomeada por meio de portaria, deverá ser atualizada sempre que houver alteração de algum dos membros.

CAPÍTULO V - AUTONOMIA

Art. 8º A ETIR-IFSULDEMINAS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto 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-IFSULDEMINAS deverá participar do processo de tomada de decisão sobre quais medidas de combate e prevenção deverão ser adotadas para que os incidentes de segurança em redes computacionais inexistam ou diminuam.

§2º A ETIR-IFSULDEMINAS 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 VI - ATRIBUIÇÕES

Art. 9º A ETIR-IFSULDEMINAS 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 caixa postal etir@ ifsuldeminas.edu.br, a ser disponibilizada pelo IFSULDEMINAS;

II - filtragem de todo conteúdo direcionado à ETIR-IFSULDEMINAS, 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 IFSULDEMINAS;

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 CSI;

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

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

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 IFSULDEMINAS.

§ 1º A ETIR-IFSULDEMINAS deverá comunicar a ocorrência de incidentes de segurança em redes de computadores ao CTIR Gov, conforme procedimentos definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal, bem como a geração de estatísticas.

§ 2º A ETIR-IFSULDEMINAS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;

§ 3º O detalhamento dos serviços prestados pela ETIR-IFSULDEMINAS deverá ser encaminhado ao Diretor de Tecnologia da Informação e ao Gestor de Segurança da Informação via ofício no sistema oficial de gestão do IFSULDEMINAS, no prazo de 30 (trinta) dias a partir da publicação da portaria com os membros da Equipe;

§ 4º A ETIR-IFSULDEMINAS deverá se reunir com periodicidade mínima de uma vez por mês, podendo realizar mais reuniões mensais de acordo com as demandas;

Art. 10º Compete ao Agente Responsável pela ETIR-IFSULDEMINAS:

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 na rede computacional do IFSULDEMINAS sejam registrados e analisados;
V - informar às autoridades competentes os assuntos relacionados a incidentes de segurança de redes computacionais;
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 IFSULDEMINAS, 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 IFSULDEMINAS. As proposições deverão ser discutidas juntamente com o Gestor de Segurança da Informação e com o Diretor de Tecnologia da Informação.

Art. 11º Compete aos membros técnicos 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 impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos; e
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.

CAPÍTULO VII - DISPOSIÇÕES GERAIS

Art. 12º A ETIR-IFSULDEMINAS deve fomentar ações de conscientização para que os servidores, colaboradores e demais usuários de sistemas de Tecnologia de Informação do IFSULDEMINAS comuniquem à ETIR-IFSULDEMINAS, o mais breve possível, toda e qualquer falha, anomalia, ameaça ou vulnerabilidade identificada, mesmo que seja apenas uma suspeita.

Art. 13º A ETIR-IFSULDEMINAS 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. 14º A ETIR-IFSULDEMINAS poderá usar as melhores práticas e soluções de mercado, desde que não conflitem com os dispositivos desta Norma Complementar ou Normas Internas do IFSULDEMINAS.

Art. 15º A troca de informações e a forma de comunicação entre a ETIR-IFSULDEMINAS e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

CAPÍTULO VIII - VIGÊNCIA

Art. 16º Esta Norma entra em vigor na data da sua publicação.

Art. 17º Os casos omissos ou não regulamentados nesta norma serão tratados pelo Comitê Gestor de Tecnologia da Informação (CGTI) do IFSULDEMINAS.

Marcelo Bregagnoli
Presidente do Conselho Superior
IFSULDEMINAS

Documento assinado eletronicamente por:

- **Marcelo Bregagnoli**, **REITOR - PRECONSUP - IFSULDEMINAS - CONSUP** , em 18/05/2022 14:30:21.

Este documento foi emitido pelo SUAP em 17/05/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 247690
Código de Autenticação: b496c4b5d4