



Universidade Federal
de São João del-Rei

PORTARIA Nº 012, DE 13 DE SETEMBRO DE 2021

Constitui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR e estabelece suas atribuições e seu escopo de atuação na Universidade Federal de São João del-Rei

O REITOR DA UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI - UFSJ, nomeado por Decreto da Presidência da República de 8 de maio de 2020, publicado no Diário Oficial da União, Seção 2 - Extra, página 1, de 8 de maio de 2020, no uso de suas atribuições legais e estatutárias, e considerando:

- a Lei 13.853 de 8 de Julho de 2019 que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providencias;

- o Decreto 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

- a Instrução normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

- a Instrução normativa nº 2, de 24 de julho de 2020, que altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal,

RESOLVE:

Art. 1º Institui, no âmbito da UFSJ, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-UFSJ.

Art. 2º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos -

ETIR-UFSJ 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 da UFSJ.

Art. 3º As atividades pertinentes à ETIR-UFSJ englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação da UFSJ 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 - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR de empresas prestadoras de serviços de tecnologia contratadas pela UFSJ;

III - as ETIRs ou estruturas equivalentes dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com a UFSJ;

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

Art. 4º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

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;

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: serviço consistente 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 da UFSJ, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.);

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

Art. 5º A implementação e o funcionamento da ETIR-UFSJ seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no "Modelo 1 - Utilizando a equipe de Tecnologia da Informação", conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados no Núcleo de Tecnologia da Informação - NTInf da UFSJ, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-UFSJ;

III - a ETIR-UFSJ ficará vinculada tecnicamente ao Setor de Internet e Redes - SETIR do NTInf;

IV - o Coordenador da ETIR-UFSJ será nomeado por ato do Presidente do Comitê Gestor de Tecnologia da Informação - CGTI;

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Chefe do Setor de Internet e Redes - SETIR.

Art. 6º A ETIR-UFSJ 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;

III - opcionais, servidores das unidades descentralizadas da UFSJ sob supervisão do

Coordenador da ETIR-UFSJ.

§ 1º Os membros da ETIR-UFSJ serão designados por meio de ato do Presidente do Comitê Gestor de Tecnologia da Informação - CGTI.

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

I - 2 (dois) servidores permanentes, oriundos do Setor de Internet e Redes;

II - 2 (dois) servidores permanentes, oriundos do Setor de Desenvolvimento de Sistemas de Informação;

III - 2 (dois) servidores permanentes, oriundos do Campus Alto Paraopeba - CAP;

IV - 2 (dois) servidores permanentes, oriundos do Campus Sete Lagoas - CSL;

V - 2 (dois) servidores permanentes, oriundos do Campus Centro Oeste Dona Lindu - CCO;

VI - 2 (dois) servidores permanentes, oriundos do Núcleo de Ensino a Distância - NEAD;

VII - 2 (dois) servidores opcionais, oriundos das unidades finalísticas da UFSJ.

Art. 7º A ETIR-UFSJ terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas da Instituição somente com anuência do Presidente do Comitê Gestor de Tecnologia da Informação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 8º A ETIR-UFSJ fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação o e-mail etir@ufsj.gov.br, a ser disponibilizado pela UFSJ;

II - filtragem de todo conteúdo direcionado à ETIR-UFSJ, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pelo NTInf, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

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

VI - resposta às solicitações e alertas encaminhados para a ETIR;

VII - A ETIR-UFSJ deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

Art. 9º Os casos omissos serão resolvidos pelo Comitê Gestor de Tecnologia da Informação da UFSJ.

Art. 10. Esta portaria entra em vigor na data de sua publicação em virtude do expediente administrativo.

A handwritten signature in blue ink, consisting of stylized, overlapping loops and lines, positioned above the printed name and title.

PROF. MARCELO PEREIRA DE ANDRADE
Reitor