UNIVERSIDADE FEDERAL DE JATAÍ
SECRETARIA EXECUTIVA E DE ÓRGÃOS COLEGIADOS

PORTARIA Nº 672/2025, DE 08 DE JULHO DE 2025

A VICE-REITORA DA UNIVERSIDADE FEDERAL DE JATAÍ, no uso das atribuições que lhe conferem o art. 11, § 1º da Lei nº 13.635, de 20 de março de 2018, bem como a Portaria Nº 90, de 31 de janeiro de 2024, publicado no Diário Oficial da União em: 1º de fevereiro de 2024, Edição: 23, Seção: 2, Páginas: 55 e 56, e no uso da competência conferida pelo art. 8º, § 2º da Lei nº 13.635, de 20 de março de 2018, c/c art. 63 do Regimento Geral da Universidade Federal de Jataí, considerando o disposto na Instrução Normativa Conjunta nº 01, de 10 de maio de 2016, do Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União, no Decreto nº 9.203, de 22 de novembro de 2017, e considerando ainda a Portaria nº 1392/2024 e tendo em vista o que consta do Processo nº 23854.010061/2024-15, RESOLVE:

Art. 1º O inciso VIII do Art. 4º da PORTARIA Nº 1392/2024, DE 19 DE DEZEMBRO DE 2024 passa a vigorar com a seguinte redação:

"Art. 4º (...) "VIII - Um membro do quadro de servidores efetivos da Universidade Federal de Jataí - UFJ, para secretariado, apoio administrativo e gerencial."

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Profa. Dra. Alana Flavia Romani
Vice-Reitora da Universidade Federal de Jataí

ANEXO - REDAÇÃO COMPILADA DA
PORTARIA Nº 1392R/2024, DE 19 DE DEZEMBRO DE 2024

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança Cibernética no âmbito da Universidade Federal de Jataí.

O REITOR DA UNIVERSIDADE FEDERAL DE JATAÍ, no uso das atribuições que lhe conferem o art. 11, § 1º da Lei nº 13.635, de 20 de março de 2018, bem como a Portaria nº 90, de 31 de janeiro de 2024, publicado no Diário Oficial da União em: 1º de fevereiro de 2024, Edição: 23, Seção: 2, Páginas: 55 e 56, e no uso da competência conferida pelo art. 8º, § 2º da Lei nº 13.635, de 20 de março de 2018, c/c art. 63 do Regimento Geral da Universidade Federal de Jataí; considerando o que consta nos Processos SEI nº 23854.006758/2023-19, nº 23854.000086/2024-19 e nº 23854.005637/2024-22; e tendo em vista a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e a Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI) e que institui o Framework de Privacidade e Segurança da Informação; **RESOLVE**:

Art. 1º Instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) com o objetivo de garantir a segurança, a integridade, a disponibilidade e a confidencialidade das informações tratadas em redes de computadores e ativos de Tecnologia da Informação e Comunicação (TIC), objetivando à preservação da infraestrutura de TIC, dados e informações e respondendo de forma eficaz a qualquer incidente cibernético que possa comprometer essas premissas na Universidade Federal de Jataí (UFJ).

§ 1º A ETIR-UFJ vincula-se à Reitoria.

§ 2º A ETIR-UFJ integra a Rede Federal de Gestão de Incidentes Cibernéticos e atua como interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR-GOV),

vinculado ao Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), do qual deve seguir todas as orientações por ele exaradas.

Art. 2º Considera-se um incidente cibernético qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, que possa comprometer a segurança, a integridade, a disponibilidade e a confidencialidade da informação; isso inclui, mas não se limita, a(o):

I - vazamento de dados confidenciais: exposição não autorizada de informações sensíveis, como dados pessoais, financeiros ou corporativos;

II - acesso não autorizado: quando um indivíduo ou grupo, interno ou externo à Universidade, obtém acesso a sistemas ou informações sem as devidas permissões;

III - ataques de negação de serviço: tentativas de tornar sistemas ou redes indisponíveis para os usuários legítimos, sobrecarregando os recursos com tráfego malicioso; e

IV - infecções por malware: inclui vírus, worms, ransomware e outros tipos de software malicioso que podem comprometer a operação de sistemas de TIC.

Art. 3º A ETIR-UFJ terá caráter permanente e atuará no âmbito da primeira linha de defesa da Instituição, consoante às definições estabelecidas na Instrução Normativa (IN) da Controladoria-Geral da União (CGU) nº 3, de 9 de junho de 2017.

Art. 4º A ETIR será representada pelos(as) titulares dos(as) seguintes órgãos/instâncias, sob coordenação do(a) primeiro(a):

I - Gestor(a) da Segurança da Informação no âmbito do PPSI, definido como Agente Responsável, conforme previsto no item 4.1 da Norma Complementar (NC) 05/IN01/DSIC/GSIPR;

II - Gestor(a) de Tecnologia da Informação no âmbito do PPSI, que ocupará a coordenação da ETIR em caso de afastamentos e impedimentos legais do membro designado no inciso I;

III - Diretor(a) da Secretaria de Tecnologia da Informação (SeTI);

IV - Coordenador(a) de Infraestrutura;

V - Coordenador(a) de Desenvolvimento;

VI - Coordenador(a) de Suporte; e

VII - Encarregado(a) de Dados, pelo Tratamento de Dados Pessoais, no âmbito da LGPD;

VIII - Um membro do quadro de servidores efetivos da Universidade Federal de Jataí - UFJ, para secretariado, apoio administrativo e gerencial.

§ 1º Os membros relacionados nos incisos de III a VI do serão representados, em suas ausências e impedimentos legais, pelo Vice-Diretor e respectivos Vice-Coordenadores ou substitutos no cargo em comissão ou função de confiança.

§ 2º Os membros da ETIR-UFJ desempenharão as atividades elencadas nesta Portaria sem prejuízo das atribuições típicas do cargo ou da função que ocupam.

§ 3º Os titulares da Diretoria de Assuntos Administrativos (DAA), Secretaria de Infraestrutura (Seinfra) e da Secretaria de Comunicação (Secom), ou seus respectivos Vice-Diretores ou substitutos no cargo em comissão ou função de confiança, atuarão como órgãos de apoio e poderão ser acionados pela ETIR-UFJ, em caso de situações que demandem ações a serem realizadas no âmbito de suas atribuições.

Art. 5º Compete à ETIR-UFJ atuar de forma preventiva e reativa para proteger a infraestrutura cibernética da UFJ, o que inclui, mas não se limita, atividades de:

I - monitoramento contínuo, por meio do acompanhamento e avaliação constantes dos sistemas e redes para identificar potenciais ameaças e vulnerabilidades;

II - análise e classificação dos incidentes com base em sua criticidade, permitindo uma resposta adequada e em tempo hábil;

III - tratamento e mitigação, por meio da adoção de medidas imediatas para dirimir os danos de incidentes cibernéticos, restaurando a normalidade o mais rapidamente possível; e

IV - emissão de alertas e/ou advertências, através da comunicação aos usuários e partes interessadas sobre vulnerabilidades e incidentes, fornecendo orientações sobre medidas de proteção e/ou correção.

Parágrafo Único. A abrangência das competências

pertinentes à ETIR-UFJ inclui os usuários (agentes públicos, colaboradores, bolsistas, terceirizados, parceiros, discentes, participantes de eventos, entre outros) e dispositivos que, ainda que temporariamente, fazem uso da infraestrutura e dos serviços de TIC da UFJ, bem como a cooperação com outras equipes técnicas, administrativas e acadêmicas, incluindo órgãos, entidades, empresas públicas ou privadas que tenham contratos, parcerias, acordos ou convênios com a Universidade.

Art. 6º A ETIR-UFJ possui as seguintes responsabilidades:

I - criar e manter estratégias de resposta a incidentes de segurança cibernética e executar as ações conforme documentado nos procedimentos internos, políticas institucionais e em boas práticas internacionais de segurança;

II - analisar, tratar e oferecer resposta a incidentes, o que abrange: receber, filtrar, classificar e responder sempre que houver algum incidente de segurança em TIC que comprometa algum ativo de rede ou serviço de TIC da UFJ no sentido de analisar o problema, decidir sobre a melhor forma para tratar e resolvê-lo tempestivamente, sempre procurando uma solução na tentativa de evitar novos incidentes;

III - tratar vulnerabilidades, o que compreende receber e analisar informações sobre vulnerabilidades em hardware e/ou software, considerando a sua natureza e as possíveis consequências aos ativos de rede e aos serviços de TIC da UFJ, visando o desenvolvimento de estratégias para a correção do problema;

IV - emitir alertas e/ou advertências, envolvendo a divulgação de informações de formas preventiva e/ou reativa alertas e/ou advertências imediatas diante de um incidente de segurança em TIC, com o objetivo de advertir e/ou dar orientações sobre como a comunidade acadêmica deve agir diante do problema;

V - divulgar de forma proativa alertas sobre vulnerabilidades ou problemas de segurança em TIC cujos impactos sejam relevantes, possibilitando, antecipadamente, que a comunidade acadêmica tenha conhecimento e orientações sobre como agir e/ou se prevenir diante de um problema, nos procedimentos internos, políticas institucionais e em boas práticas internacionais de segurança;

VI - elaborar relatórios de incidentes de segurança

cibernética;

VII - investigar, em conjunto com demais unidades acadêmicas e/ou administrativas, a partir das informações registradas, as possíveis causas e extensões do incidente;

VIII - oferecer resposta eficiente, adequada e proporcional aos incidentes cibernéticos que apresentem risco à integridade, disponibilidade ou confidencialidade das informações hospedadas na rede de computadores e nos ativos de TIC;

IX - propor plano(s) de contingência e acompanhar a execução de ações de contenção do incidente, aprimorando-o(s), quando necessário;

X - indicar a necessidade de aperfeiçoamento de controles de segurança para limitar a frequência, os danos e o custo de futuras falhas de funcionamento dos serviços e ativos de TIC;

XI - coletar e preservar as evidências digitais em incidentes cibernéticos penalmente relevantes, conforme legislações vigentes;

XII - elaborar, promover e disseminar práticas de segurança em TIC no âmbito da Universidade; e

XIII - documentar os eventos tratados de forma a constituir um banco de conhecimento para apoio em eventos futuros, contendo informações sobre o ocorrido, as causas e a(s) solução(ões) adotada(s).

Parágrafo Único. Havendo indícios de ilícitos criminais, a ETIR-UFJ deve informar às autoridades policiais competentes, por meio de registro de boletim de ocorrência, para a adoção dos procedimentos criminais e/ou legais julgados necessários, sem prejuízo ao disposto no item 10.6 da NC nº 05/IN01/DSIC/GSIPR e do item 6 da NC nº 08/IN01/DSIC/GSIPR, encaminhando cópia do boletim ao Comitê Estratégico de Governança, Riscos e Controles.

Art. 7º A ETIR deve elaborar relatório técnico com periodicidade trimestral sobre os incidentes de segurança cibernética contendo, no mínimo, as seguintes informações:

I - ações preventivas realizadas no trimestre;

II - quantitativo e descrição dos incidentes cibernéticos confirmados e que estiveram sob suspeita;

III - criticidades dos incidentes, baseada nos impactos identificados;

IV - descrição sobre as causas dos incidentes;

V - listagem das informações comprometidas, se houver; e

VI - descrição sobre as medidas de solução adotadas.

§ 1º O aludido relatório técnico deve ser submetido pela Coordenação da ETIR às Presidências do Comitê de Gestão de Processos e Riscos e do Comitê de Gestão Integrada de Dados e Segurança da Informação até o quinto dia útil do mês subsequente.

§ 2º As Presidências dos Comitês citados no parágrafo 1º deste artigo deverão analisar o relatório com as respectivas equipes e realizar o tratamento das informações nele expostas no âmbito das respectivas responsabilidades, de modo a contribuir com os objetivos estabelecidos nesta Portaria.

§ 3º As referidas Presidências deverão elaborar relatório consolidado com os principais incidentes de segurança ocorridos na periodicidade prevista no caput e encaminhá-lo ao Comitê Estratégico de Governança, Riscos e Controles até o quinto dia útil do mês subsequente ao recebimento do relatório técnico, para tratativas concernentes às atribuições do comitê estratégico.

Art. 8º Fica estabelecido o prazo de 30 (trinta) dias, a contar da data da publicação desta Portaria, para a criação do sítio eletrônico específico da ETIR, contendo, no mínimo, a publicação de canal(is) de contato(s), competências, responsabilidades e da respectiva portaria que a instituiu, bem como para ampla divulgação à comunidade acadêmica acerca das informações dispostas nesta Portaria.

Art. 9º Durante o tratamento de incidentes, a ETIR-UFJ tem autonomia completa para tomar as medidas técnico-operacionais emergenciais necessárias para o restabelecimento dos serviços com vistas à manutenção e à recuperação da segurança, da integridade, da disponibilidade e da confidencialidade dos dados, informações, dos sistemas e da rede da Universidade.

Parágrafo Único. A ETIR tem autonomia para solicitar apoio multidisciplinar de quaisquer unidades acadêmica e/ou administrativa, sobretudo às áreas de Infraestrutura, Assuntos

Administrativos e de Comunicação, conforme previsto no Parágrafo 2º do art. 4º, para responder aos incidentes de maneira adequada e tempestiva.

Art. 10. Ficam revogadas disposições em contrário.

Art. 11. Os casos omissos serão resolvidos pela Reitoria.

Art. 12. Esta portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **ALANA FLAVIA ROMANI**, **Vice-Reitora da Universidade Federal de Jataí/UFJ**, em 08/07/2025, às 16:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufj.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0450907** e o código CRC **C5A80B24**.

Referência: Processo nº 23854.010061/2024-15

SEI nº 0450907