PORTARIA Nº 003/2026

O VICE-REITOR NO EXERCÍCIO DO CARGO DE REITOR DA UNIVERSIDADE FEDERAL DO SUL DA BAHIA, no uso de suas atribuições regimentais e estatutárias, bem como considerando suas atribuições como Presidente do Comitê de Governança Digital e de Segurança da Informação (CGDSI), conforme Art. 2º, inciso II da Resolução nº 21, de 27 de novembro de 2025,

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados Pessoais – LGPD;

CONSIDERANDO o Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal;

CONSIDERANDO a Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, que institui o Programa de Privacidade e Segurança da Informação no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o SISP;

CONSIDERANDO a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

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

CONSIDERANDO a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;

CONSIDERANDO a Portaria DSI/GSI/PR nº 120, de 21 de dezembro de 2022, que aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal;

CONSIDERANDO a Norma Complementar IN01/DSIC/GSIPR nº 5, de 14 de agosto de 2009, que dispõe sobre a criação de equipes de tratamento e resposta a incidentes em redes computacionais;

CONSIDERANDO a Norma Complementar IN01/DSIC/GSIPR nº 8, de 19 de agosto de 2010, que dispõe sobre as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da administração pública federal.

RESOLVE:

Art. 1º Instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança Cibernética da Universidade Federal do Sul da Bahia (ETIR-UFSB), de caráter permanente e definir seu escopo de atuação.

Art. 2º A ETIR-UFSB tem por finalidade promover a prevenção, o tratamento e a resposta a incidentes cibernéticos, visando proteger os ativos de Tecnologia da Informação e Comunicação (TIC) e reduzir impactos operacionais e institucionais, observando os normativos aplicáveis.

Art. 3º A ETIR-UFSB vincula-se à Superintendência de Tecnologia da Informação (STI), com reporte ao Comitê de Governança Digital e de Segurança da Informação (CGDSI) para fins de orientação, acompanhamento e governança de suas atividades e entregas.

§ 1º O/A Gestor(a) de Segurança da Informação atua como instância de reporte e decisão, em regime de autonomia compartilhada, especialmente nos incidentes relevantes e nas deliberações que extrapolem o âmbito técnico-operacional.

§ 2º Compete ao/à Gestor(a) de Segurança da Informação, em articulação com a STI, garantir a capacitação continuada, a disponibilidade de recursos e o escalonamento às instâncias competentes, quando necessário, para o adequado funcionamento da ETIR-UFSB.

Art. 4º Os incidentes relevantes, assim classificados conforme critérios definidos no Plano de Resposta a Incidentes da UFSB, serão imediatamente escalonados à Reitoria e ao/à Gestor(a) de Segurança da Informação, sem prejuízo do reporte ao CGDSI e das comunicações cabíveis.

§ 1º Quando o incidente envolver ou puder envolver dados pessoais, a ETIR-UFSB deverá comunicar imediatamente o/a Encarregado/a de Dados (DPO) da UFSB, para avaliação conjunta do impacto e das medidas de contenção, mitigação e comunicação.

§ 2º A comunicação à ANPD, quando aplicável, será realizada por intermédio do/a DPO, observadas as orientações e os procedimentos vigentes para Comunicado de Incidente de Segurança (CIS).

Art. 5º A ETIR-UFSB 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), e com o Centro de Atendimento a Incidentes de Segurança (CAIS/RNP), observadas as orientações emitidas por essas instâncias.

Art. 6º Considera-se 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. 7º A ETIR-UFSB será composta por membros indicados pela STI, designados em ato próprio, observada, preferencialmente, a representação das seguintes áreas:

I. Infraestrutura e conectividade;
II. Arquitetura de redes e serviços;
III. Sistemas e aplicações;
IV. Segurança da informação;
V. Suporte ao usuário e operação/monitoramento.

§ 1º A composição nominal, bem como eventuais substituições, serão formalizadas por Portaria do Gabinete da Reitoria, mediante indicação da STI e comunicação ao CGDSI.

§ 2º O/A Gestor(a) de Segurança da Informação atuará como instância de reporte e decisão (autonomia compartilhada), não integrando a composição nominal de membros da ETIR-UFSB, e apoiará seu funcionamento mediante a garantia de capacitação, recursos e escalonamento, em articulação com a STI e CGDSI.

Art. 8º Compete a ETIR-UFSB atuar de forma preventiva e reativa para proteger a infraestrutura cibernética da UFSB, 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-UFSB 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 UFSB, 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. 9º A ETIR-UFSB 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 UFSB 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 UFSB, 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).

XIV. articular-se com o/a Encarregado/a de Dados (DPO) nos incidentes que envolvam dados pessoais, fornecendo informações técnicas necessárias à avaliação e às comunicações legais e regulatórias cabíveis.

Parágrafo único: Havendo indícios de ilícitos criminais, a ETIR-UFSB 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 Norma Complementar nº 05/IN01/DSIC/GSIPR e do item 6 da Norma Complementar nº 08/IN01/DSIC/GSIPR, encaminhando cópia do boletim ao CGDSI.

Art. 10 A ETIR-UFSB deve elaborar relatório técnico com periodicidade trimestral sobre os incidentes de segurança cibernética contendo, no mínimo, as seguintes informações:

I. ações preventivas realizadas no semestre;
II. quantitativo e descrição dos incidentes cibernéticos 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 relatório técnico deve ser submetido ao CGDSI até o quinto dia útil do mês subsequente.

§ 2º O CDGSI deverá analisar o relatório e realizar o tratamento das informações nele expostas no âmbito das respectivas responsabilidades, de modo a contribuir com os objetivos estabelecidos nesta Portaria.

Art. 11 Fica estabelecido o prazo de 60 (sessenta) dias, a contar da data de 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. 12 Durante o tratamento de incidentes, a ETIR-UFSB tem autonomia técnico-operacional para tomar as medidas 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-UFSB tem autonomia para solicitar apoio multidisciplinar de quaisquer unidades acadêmica e/ou administrativa para responder aos incidentes de maneira adequada e tempestiva.

Art. 13 Ficam revogadas disposições em contrário.

Art. 14 Os casos omissos serão resolvidos pelo(a) Gestor(a) de Segurança da Informação em articulação com o CGDSI.

Art. 15 Esta portaria entra em vigor na data de sua publicação.

Itabuna, 08 de janeiro de 2026

FRANCISCO JOSÉ GOMES MESQUITA
VICE-REITOR NO EXERCÍCIO DO CARGO DE REITOR