UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

INSTRUÇÃO NORMATIVA PROTIC/UFOB Nº 001/2026, DE 04 DE AGOSTO DE 2026

Estabelece o Plano de Resposta a Incidentes de Segurança da Informação da Universidade Federal do Oeste da Bahia – UFOB.

O PRÓ-REITOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, nomeado pela portaria nº 282, de 17 de outubro de 2023, publicada no Diário Oficial da União nº 198 de 18 de outubro de 2023, seção 2, no uso de suas atribuições legais, resolve:

Art. 1º Estabelecer o Plano de Resposta a Incidentes de Segurança da Informação - PRISI da Universidade Federal do Oeste da Bahia.

§1º O PRISI tem por objetivo:

I. assegurar a continuidade dos serviços de TIC;
II. implementar um processo para conter efetivamente o impacto e a presença de ameaças;
III. restaurar a integridade da rede e dos sistemas da organização; e
IV. proteger os dados institucionais e pessoais.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º Para efeitos desta Instrução Normativa, considera-se:

I. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

II. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores);

III. Autoridade Nacional de Proteção de Dados (ANPD): os Arts. 5° inciso XIX, 55-A e seguintes da LGPD definem a Autoridade Nacional de Proteção de Dados (ANPD) como Autarquia de Natureza Especial, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018 - LGPD em todo o território nacional, conforme as

atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020;

IV. CTIR Gov: o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) é integrante do Departamento de Segurança de Informação e Cibernética (DSIC) da Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR). Tem o papel de coordenar e integrar as ações destinadas à gestão de incidentes de TI em órgãos e entidades da Administração Pública Federal (APF). Os incidentes de segurança e de privacidade estão inclusos no escopo de ação do CTIR. Em caso de incidentes de segurança em redes computacionais, devem-se observar as diretrizes constantes na Norma Complementar nº 21/IN01/DSIC/GSIPR, que trata do registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes;

V. Dados pessoais: toda informação relacionada a pessoa natural identificada ou identificável;

VI. Dados pessoais sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

VII. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VIII. Endereço IP: conjunto de elementos numéricos ou alfanuméricos, que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

IX. Engenharia Social: técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;

X. ETIR: Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos internos de órgãos da Administração Pública Federal (APF);

XI. Incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XII. Incidente com Dados em Larga Escala: de acordo com a ANPD, incidente com dados em larga escala é aquele que abrange um número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

XIII. Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XIV. Incidente de Segurança com Dados Pessoais: de acordo com a ANPD, é um evento adverso confirmado que compromete a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados;

XV. LGPD: Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo.

XVI. IP: sigla de *Internet Protocol;*

XVII. Log: registro de eventos relevantes em um dispositivo ou sistema computacional;

XVIII. Malware: software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans(ou cavalos de Troia), spyware, adware e rootkits;

XIX. Máquinas Virtuais: são computadores de *software* com as mesmas funcionalidades que os computadores físicos. Assim como os computadores físicos, elas executam aplicativos e um sistema operacional. No entanto, as máquinas virtuais são arquivos de computador, executados em um computador físico, e se comportam como um computador físico. Geralmente, são criadas para tarefas específicas, cujas execuções são arriscadas em um ambiente *host,* como por exemplo, o acesso a dados infectados por vírus e a testes de sistemas operacionais. Como a máquina virtual é separada por *sandbox* do restante do sistema, o *software* dentro dela não pode adulterar o computador *host*. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores;

XX. Phishing: é um tipo de fraude na qual o golpista tenta obter informações pessoais e financeiros do usuário, combinando meios técnicos e engenharia social;

XXI. RIPD: conforme a LGPD, o Relatório de Impacto a Proteção de Dados (RIPD) é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos

fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XXII. Relatório Final: relatório que contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas;

XXIII. Snapshot: Um registro do estado de um arquivo, aplicação ou sistema em certo ponto no tempo,

XXIV. Sniffing: corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um sniffer (aplicativo destinado a capturar pacotes de rede);

XXV. Spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

XXVI. Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

XXVII. Worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

CAPÍTULO II

DA NOTIFICAÇÃO

Art. 3º A notificação de incidentes de segurança da informação relacionados à rede computacional ou aos ativos da instituição deverá ser realizada à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), por meio de um dos seguintes canais institucionais:

I. abertura de solicitação diretamente no sistema da Central de Atendimento ao usuário de TIC, Veredas, disponível no endereço https://veredas.ufob.edu.br;

II. preenchimento de formulário eletrônico específico, disponível no Catálogo de Serviços de TIC da UFOB, no seguinte endereço: https://ufob.edu.br/a-ufob/servicos/tic; ou

III. envio de mensagem para o e-mail: etir@ufob.edu.br.

Art. 4º Os canais previstos nos incisos II e III do art. 3º estarão disponíveis para a comunicação de incidentes de segurança da informação por órgãos externos e pelo público em geral, inclusive aqueles que não possuam acesso institucional à rede da UFOB.

Art. 5º Recomenda-se que a notificação contenha uma descrição detalhada da ocorrência com artefatos que possibilitem evidenciar o incidente.

CAPÍTULO III

DA TRIAGEM

Art. 6º A primeira etapa do processo de tratamento e resposta a incidentes de segurança, após sua notificação ou detecção pela ETIR, será a triagem.

Parágrafo único. A triagem terá por finalidade reunir e analisar as informações necessárias à caracterização do incidente, considerando sua abrangência, correlação, prioridade, registro e atualização.

Art. 7º A abrangência definirá se a ocorrência se caracteriza como incidente de segurança cibernética.

Parágrafo único. Caso se constate que a ocorrência não está no âmbito do escopo de atuação da ETIR, a demanda deverá ser redirecionada ao responsável ou setor competente para o devido atendimento.

Art. 8º A correlação verificará se existe relacionamento com outros incidentes já ocorridos ou em tratamento.

Art. 9º A ETIR classificará o incidente conforme a categoria mais compatível com o vetor de ataque, objetivo ou ativo de destino.

Parágrafo único. As categorias podem sofrer atualizações conforme necessidade e não exclusivamente serão definidas por:

I. Conteúdo abusivo: Spam, correntes, entre outros;

II. Código malicioso: worm, vírus, bots, trojan, spyware, scripts maliciosos;

III. Pesquisa por informações: varredura, sniffing, engenharia social;

IV. Tentativa de intrusão: tentativas de login não autorizadas, ataques de força bruta;

V. Indisponibilidade de serviço: negação de serviço, sabotagem;

VI. Fraude: violação de software, acesso ilegítimo com credenciais institucionais, uso de recursos de TIC de forma não-autorizada;

VII. Vulnerabilidades: serviço mal configurado, bugs e falhas de software ou hardware; e

VIII. Outros: Categorias de Incidentes não listados abaixo.

Art. 10. A priorização para atendimento do incidente será definida considerando a classificação, as informações obtidas inicialmente e o conhecimento técnico da ETIR, de acordo com um dos seguintes níveis de gravidade:

I. Alta: incidentes críticos e com impacto significativo nas operações da Universidade, na segurança de dados e na integridade dos sistemas, exigem ação imediata. Exemplos incluem ataques de negação de serviço que derrubam a rede da Universidade ou um incidente com dados em larga escala.

II. Média: incidentes que causam impactos moderados e podem afetar a operação de partes da Universidade, mas não comprometem serviços essenciais nem causam grandes danos à instituição. Exemplos incluem phishing enviado para um grande número de usuários ou indisponibilidade de um ativo de rede compartilhado por vários usuários.

III. Baixa: incidentes que são de fácil resolução e podem não necessitar de uma investigação aprofundada. Exemplos incluem situações como a presença de malware em um único computador ou um incidente de perda de senha, possui impacto mínimo nas operações da Universidade.

Art. 11. A ETIR deverá utilizar sistema Central de Atendimento aos usuários de TIC para relatar as informações tratadas.

§1º A atualização de processamento deverá ser gerenciada durante todo o ciclo de vida do incidente.

§2º Um ou mais agentes da ETIR podem ser designados para o atendimento, sendo responsáveis por atualizar as informações.

CAPÍTULO IV

DA DETECÇÃO E ANÁLISE

Art. 12. A etapa de detecção e análise consiste no conjunto de atividades que devem ser executadas para a obtenção de mais detalhes sobre o incidente recebido e possibilitar ações de resposta.

§1º A ETIR validará as informações recebidas na triagem, complementando-as ou retificando-as, quando necessário;

§2º A ETIR identificará, sempre que possível, atividades que apresentem comportamento anômalo em relação à linha de base conhecida, observando, quando aplicável, no mínimo:

I. Fluxos de dados;

II. Logs de acesso;

III. Utilização de recursos computacionais e métricas de servidores;

IV. Endereços IP e portas de comunicação;

V. Histórico de comandos; e

VI. Autenticação de usuários.

§3º A ETIR identificará, sempre que possível, elementos da cadeia de ataque que possam subsidiar a definição das ações de resposta, podendo, quando necessário, utilizar outras fontes para descoberta de informação, observando ferramentas e frameworks adequados;

Art. 13. A ETIR da UFOB será o ponto central de comunicação com o CTIR Gov, como estratégia de colaboração para a resolução e registro de incidentes cibernéticos.

Art. 14. Em caso de vazamento de dados pessoais, o incidente deverá ser comunicado ao Encarregado pelo Tratamento de Dados Pessoais da UFOB, pelo e-mail: protecao.dados@ufob.edu.br.

CAPÍTULO V

DAS ATIVIDADES DE RESPOSTA

SEÇÃO I

DO PLANEJAMENTO DAS AÇÕES

Art. 15. As atividades de resposta visam a contenção, erradicação e recuperação dos sistemas afetados.

Art. 16. Caso exista Plano de Continuidade de Negócios aplicável aos sistemas impactados, deverão ser observadas as ações nele previstas.

Art. 17. As ações de resposta devem levar em consideração os seguintes critérios:

I - criticidade dos ativos;

II - tipo e gravidade do incidente;

III - os recursos necessários para a preservação das evidências;

IV - importância dos sistemas e dados afetados para os processos de negócio essenciais; e

V - recursos necessários para implementar a estratégia de resposta.

Art. 18. Deve-se preservar as evidências de acessos e qualquer alteração que possua relação com o sistema ou conjuntos de dados afetados.

Art. 19. Em caso de incidente com máquinas virtuais, pode ser feito o registro do estado em que se encontram os sistemas, aplicações ou arquivos através de snapshot para análise.

SEÇÃO II

DAS AÇÕES DE CONTENÇÃO

Art. 20. São atividades de contenção que podem ser consideradas pela execução:

I - interrupção de acesso a sistemas, arquivos ou bases de dados do público em geral;

II - isolamento de segmentos de rede;

III - alteração de políticas de roteamento;

IV - bloqueio de padrões de tráfego ou endereços suspeitos;

V - isolamento de dispositivos que estejam infectados com malware ou possam causar comprometimento de outros dispositivos da rede;

VI - Desabilitar serviços vulneráveis; e

VII - Suspensão de contas institucionais com indícios de comprometimento.

Art. 21. As medidas de contenção podem mitigar o incidente, para evitar danos maiores a terceiros e a perda de informação relevante que pode ser necessária para processo cível, penal ou administrativo.

SEÇÃO III

DAS AÇÕES DE ERRADICAÇÃO

Art. 22. São atividades de erradicação que podem ser consideradas para a execução:

I - restauração de imagens completas de unidades de armazenamento;

II - recuperação de dados e sistemas a partir de backups íntegros;

III - realização de procedimentos para remoção dos artefatos utilizados por atacantes ou ferramentas de remoção de software mal-intencionado; e

IV - correção de vulnerabilidades encontradas.

SEÇÃO IV

DAS AÇÕES DE RECUPERAÇÃO

Art. 23. O objetivo da recuperação é restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas.

Art. 24. As atividades de recuperação podem conter:

I - definição de cronograma para restauração das operações junto aos responsáveis dos ativos de informação afetados;

II - realizar varredura completa no ambiente afetado;

III - realização de testes de funcionamento; e

IV - monitoramento do ambiente recuperado.

CAPÍTULO VI

DAS ATIVIDADES PÓS-INCIDENTE

Art. 25. As atividades de pós-incidente serão executadas pela ETIR em busca do aprendizado e melhoria do processo de resposta a incidentes.

Art. 26. O Relatório Final deverá descrever as ações realizadas para resolução do incidente juntamente com informações adicionadas em seu ciclo de vida em resposta aos seguintes requisitos:

I - circunstâncias do incidente: onde ocorreu, quem o reportou (se não for anônimo) e como foi descoberto;

II - a causa do incidente;

III - as vulnerabilidades exploradas;

IV - se houve o uso de credenciais comprometidas, identificando-as;

V - os sistemas, equipamentos e redes comprometidos;

VI - os setores da Universidade afetados;

VII - se houve exposição, transferência ou sequestro de dados;

VIII - se houve dados pessoais, quais dados e titulares foram afetados;

IX - as medidas adotadas para contenção, erradicação e recuperação;

X - as lições aprendidas; e

XI - encaminhamento para instâncias competentes para que sejam tomadas as providências cabíveis, quando se fizer necessário.

Art. 27. A ETIR deverá confirmar que a causa raiz foi eliminada ou mitigada.

Art. 28. É desejável que reuniões sejam realizadas após a ocorrência de incidentes, especialmente os que forem mais críticos ou reuniões periódicas para avaliação geral dos acontecimentos.

Art. 29. Estabelecer, sempre que necessário, comunicação com o Comitê Permanente de Segurança da Informação e Órgão de TIC da UFOB para alinhamento das estratégias de prevenção, tratamento e resposta aos incidentes.

CAPÍTULO VII

DO INCIDENTE COM DADOS PESSOAIS

Art. 30. No caso de incidente de segurança com dados pessoais e dados pessoais sensíveis o presente Plano aponta, dentro do fluxo de tratamento de incidentes da ETIR - UFOB, as seguintes medidas como fundamentais:

I. avaliação interna do incidente: procurar responder às questões iniciais sobre impacto do evento, natureza, categoria, quantidade de titulares e dados pessoais afetados, consequências para Universidade e titulares;

II. comunicação ao Encarregado da LGPD da UFOB da existência do incidente para execução de medidas cabíveis e comunicação aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD);

III. comunicação ao Controlador da existência do incidente;

IV. comunicar ao CTIR Gov; e

V. emitir o relatório final com todas as informações coletadas necessárias para promover a melhoria contínua e fornecer subsídios para atualização do Relatório de Impacto a Proteção de Dados (RIPD) pelo Controlador.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 31. Esta Instrução Normativa entra em vigor na data de sua publicação no Boletim de Serviços da UFOB.

Art. 32. Os casos omissos serão dirimidos pela Pró-Reitoria de Tecnologia da Informação e Comunicação.

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

Documento assinado digitalmente
UILIAM RANGEL AMORIM SOUZA
Data: 04/08/2026 16:14:32-0300
Verifique em https://validar.iti.gov.br

Uiliam Rangel Amorim Souza

Pró-Reitor de Tecnologia da Informação e Comunicação

Documento assinado digitalmente
CLEYTON MARTINS SENA
Data: 05/08/2026 15:37:01-0300
Verifique em https://validar.iti.gov.br

Cleyton Martins Sena

Gestor de Segurança da Informação