UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Gabinete da Reitoria

PORTARIA UFOB N° 667, DE 21 DE MAIO DE 2026

Institui o Manual de Comunicação de Incidentes de Segurança com Dados Pessoais.

O REITOR DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, nomeado pelo Decreto de 11 de setembro de 2023, publicado no Diário Oficial da União em 12 de setembro de 2023, seção 2, pág. 1, tendo em vista o disposto no art. 8º da Lei nº 12.825, de 5 de junho de 2013, no uso das atribuições que lhe conferem no art. 51 do Regimento Geral da UFOB, resolve:

Art. 1º Instituir o Manual de Comunicação de Incidentes de Segurança com Dados Pessoais, conforme anexo I.

Art. 2º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviços da UFOB.

JACQUES ANTONIO DE MIRANDA

Reitor

gov.br
Documento assinado digitalmente
JACQUES ANTONIO DE MIRANDA
Data: 21/05/2026 16:59:58-0300
Verifique em https://validar.iti.gov.br

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

UFOB

UNIVERSIDADE FEDERAL
DO OESTE DA BAHIA

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

BARREIRAS – BA

2026

Ministério da Educação

Universidade Federal do Oeste da Bahia

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

Manual institucional de governança, análise, registro e comunicação de incidentes envolvendo dados pessoais no âmbito da Universidade Federal do Oeste da Bahia

Barreiras – BA

2026

REITORIA 2023 - 2027

Reitor
Jacques Antonio de Miranda

Vice-Reitor
Antonio Oliveira de Sousa

Chefe de Gabinete
Marina Meirelles Paes

Pró-Reitora de Administração
Jaqueline Fritsch

Pró-Reitor de Extensão e Cultura
Anderson Breno Souza

Pró-Reitora de Graduação
Adma Katia Lacerda Chaves

Pró-Reitor de Gestão de Pessoas
Clayton da Silva Barcelos

Pró-Reitor de Planejamento e Desenvolvimento Institucional
Leriane Silva Cardozo

Pró-Reitora de Pós-Graduação e Pesquisa
Aurizangela Oliveira de Sousa

Pró-Reitor de Tecnologia da Informação e Comunicação
Uiliam Rangel Amorim Souza

Pró-Reitor de Ações Afirmativas e Assuntos Estudantis
Antonio Oliveira de Sousa

Secretária Acadêmica
Leila Oliveira dos Anjos

Superintendente Administrativa do Campus Reitor Edgard Santos
Marcus Vinicius Soares Figueiredo Castro Silva

Superintendente de Inovação e Tecnologia para o Desenvolvimento Regional
Erick Samuel Rojas Cajavilca

Diretor de Governança, Riscos e Conformidade
Angelo Marconi Maniero

Diretor de Comunicação Institucional e Científica
Danilo de Azevedo Pinto

Diretora de Saúde Universitária
Taíse de Oliveira Silva

Auditor-Chefe
Mariano Ramalho de Andrade Segundo

Ouvidora
Liliane Maria Reis Marcon

Corregedora
Fabiana de Carvalho Calixto

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Reinilton da Silva Juvenal

COMITÊ PARA IMPLEMENTAÇÃO DA LGPD NA UFOB

Diretor de Governança, Riscos e Conformidade
Angelo Marconi Maniero (presidente)

Coordenador de Gestão Estratégica
Reinilton da Silva Juvenal (vice-presidente)

Diretor de Comunicação Institucional e Científica
Danilo de Azevedo Pinto

Secretária Acadêmica
Leila Oliveira dos Anjos

Ouvidora
Liliane Maria Reis Marcon

Coordenador de Governança e Atendimento
Pedro Fernandes Felipe

Coordenador de Sistemas da Informação
Yan Kaic Antunes da Silva

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR-UFOB)

Gestor de Segurança da Informação
Cleyton Martins Sena (coordenador)

Gestor do Núcleo de Segurança da Informação
Elivelton de Oliveira Santos (coordenador substituto)

Pró-Reitor de Tecnologia da Informação e Comunicação
Uiliam Rangel Amorim Souza

Coordenador de Governança e Atendimento
Pedro Fernandes Felipe

Coordenador de Infraestrutura e Segurança
Luiz Hilário Ferreira Damascena

Coordenador de Sistemas da Informação
Yan Kaic Antunes da Silva

DIRETORIA DE GOVERNANÇA, RISCOS E CONFORMIDADE

Diretor de Governança, Riscos e Conformidade
Angelo Marconi Maniero

Coordenadora de Riscos e Conformidade
Vanessa Godoy Kinoshita

Núcleo de Conformidade de Normativos
Odalicio de Oliveira Alves

SUMÁRIO

1. CONTEXTO

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece que os agentes de tratamento devem adotar medidas aptas à proteção dos dados pessoais e à prevenção de danos aos titulares decorrentes de incidentes de segurança. Nos termos do art. 48 da LGPD, o controlador deverá comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A matéria foi regulamentada pela Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança, estabelecendo critérios, procedimentos e prazos aplicáveis à comunicação de incidentes de segurança envolvendo dados pessoais. O Tribunal de Contas da União, por meio do Acórdão nº 1372/2025 – TCU – Plenário, determinou às organizações fiscalizadas, dentre elas a Universidade Federal do Oeste da Bahia (UFOB), a adoção de medidas destinadas à implementação de modelo de comunicação de incidentes de segurança à ANPD e aos titulares de dados pessoais, nos termos da LGPD.

Diante desse contexto, o presente Manual de Comunicação de Incidente de Segurança da Informação com Dados Pessoais tem por objetivo estabelecer, no âmbito da UFOB, o fluxo institucional de identificação, análise, registro e comunicação de incidentes de segurança envolvendo dados pessoais, em alinhamento com a LGPD, com a Resolução CD/ANPD nº 15/2024 e com a Política de Segurança da Informação da UFOB.

O manual observa a estrutura de governança prevista na Resolução CGAG/CONSUNI/UFOB nº 018/2023, que instituiu a Política de Segurança da Informação da UFOB. Observa, ainda, as competências atribuídas à Equipe de Prevenção,

Tratamento e Resposta a Incidentes Computacionais (ETIR-UFOB), regulamentada pela Portaria PROTIC/UFOB nº 02/2024.

A avaliação quanto à necessidade de comunicação do incidente deverá observar os critérios de risco ou dano relevante aos titulares previstos na Lei nº 13.709/2018 e na Resolução CD/ANPD nº 15/2024, não se presumindo a obrigatoriedade de comunicação em todo e qualquer incidente de segurança.

A proposta foi elaborada no âmbito do Comitê de Implementação da Lei Geral de Proteção de Dados na UFOB, instituído pela Portaria UFOB nº 220, de 15 de março de 2021, com participação das unidades institucionais envolvidas nas atividades de governança, segurança da informação, tecnologia da informação, comunicação institucional e proteção de dados pessoais.

2. DEFINIÇÕES

Para fins de aplicação deste Manual de Comunicação de Incidente de Segurança da Informação com Dados Pessoais, consideram-se as seguintes definições:

AGENTES DE TRATAMENTO: o controlador e o operador.

AMPLA DIVULGAÇÃO DO INCIDENTE EM MEIOS DE COMUNICAÇÃO: providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do controlador ou em outros meios de comunicação;

AUTENTICIDADE: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

CATEGORIA DE DADOS PESSOAIS: classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA: ato pelo qual o controlador comunica à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos do *caput* do art. 48 da Lei nº 13.709/2018;

CONFIDENCIALIDADE: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados;

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito deste

manual, o controlador é a Universidade Federal do Oeste da Bahia, por ser a entidade pública responsável pelas decisões institucionais sobre o tratamento de dados pessoais no exercício de suas competências legais.

DADO DE AUTENTICAÇÃO EM SISTEMAS: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de *login*, *tokens* e senhas;

DADO FINANCEIRO: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

DADO PESSOAL AFETADO: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;

DADO PESSOAL SENSÍVEL: dado pessoal 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;

DADO PROTEGIDO POR SIGILO LEGAL OU JUDICIAL: dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;

DADO PROTEGIDO POR SIGILO PROFISSIONAL: dado pessoal cujo sigilo decorra do exercício de função, cargo de direção, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

DADOS EM LARGA ESCALA: dados relacionados a número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento;

DISPONIBILIDADE: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;

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.

GESTOR DA BASE DE DADOS: unidade organizacional responsável pela guarda, manutenção ou utilização da base de dados que contenha os dados pessoais afetados pelo incidente, nos termos do art. 16 da Política de Segurança da Informação (Resolução CGAG/CONSUNI/UFOB nº 18/2023);

INCIDENTE DE SEGURANÇA: qualquer evento adverso confirmado relacionado ao comprometimento das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais;

INTEGRIDADE: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental;

MEDIDAS DE SEGURANÇA: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

NATUREZA DOS DADOS PESSOAIS: classificação de dados pessoais em gerais ou sensíveis;

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

RELATÓRIO DE TRATAMENTO DO INCIDENTE: documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos;

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

3. DA GOVERNANÇA E DO FLUXO INSTITUCIONAL DE ATUAÇÃO

A gestão de incidentes de segurança envolvendo dados pessoais observará a estrutura de governança estabelecida na Resolução CGAG/CONSUNI/UFOB nº 018/2023 (Política de Segurança da Informação), na Portaria PROTIC/UFOB nº 02/2024, que regulamenta a ETIR-UFOB, e na Lei nº 13.709/2018 (LGPD), constituindo o presente instrumento mecanismo de organização do fluxo institucional de atuação.

No âmbito desse fluxo institucional:

I. compete à ETIR-UFOB:

a) identificar e registrar o incidente;

b) realizar análise técnica e classificação preliminar;

c) adotar medidas de contenção, mitigação e recuperação;

d) preservar evidências e apoiar a apuração técnica;

e) atuar de forma integrada com as unidades envolvidas.

II. compete ao gestor da base de dados afetada:

a) prestar informações sobre a natureza dos dados pessoais envolvidos;

b) informar a finalidade do tratamento e a abrangência dos titulares afetados;

c) auxiliar na avaliação dos impactos institucionais e operacionais decorrentes do incidente.

III. compete ao Encarregado pelo tratamento de dados pessoais:

a) coordenar o fluxo institucional de análise e comunicação do incidente;

b) avaliar a caracterização do incidente de segurança envolvendo dados pessoais;

c) avaliar a existência de risco ou dano relevante aos titulares;

d) decidir quanto à necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares;
e) realizar as comunicações legalmente exigidas;

IV. o(a) Reitor(a) será cientificado(a) da ocorrência do incidente e das medidas adotadas no âmbito da resposta institucional.

As medidas de análise, contenção, mitigação, registro e comunicação poderão ser realizadas com base nas informações disponíveis no momento da avaliação, ainda que preliminares, devendo os registros e documentos correspondentes ser complementados posteriormente, conforme a evolução das apurações técnicas e administrativas.

As informações relativas ao incidente, às análises realizadas, às decisões adotadas e às comunicações efetuadas deverão ser registradas no processo administrativo correspondente.

4. DA CARACTERIZAÇÃO DO INCIDENTE E DA NECESSIDADE DE COMUNICAÇÃO

A comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares será realizada nos casos de incidente de segurança envolvendo dados pessoais que possa acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 15/2024.

A avaliação quanto à existência de risco ou dano relevante deverá considerar, de forma conjunta, as circunstâncias do caso concreto, especialmente:

I. a natureza e a sensibilidade dos dados pessoais envolvidos;
II. a categoria dos titulares potencialmente afetados;
III. a possibilidade de identificação dos titulares;
IV. o volume de dados e a quantidade de titulares afetados;
V. o tipo de incidente ocorrido;
VI. os potenciais impactos aos titulares, inclusive quanto a prejuízos financeiros, discriminação, danos reputacionais, violação de direitos ou comprometimento da segurança dos titulares;
VII. o alcance do incidente, considerando sua extensão institucional ou externa;
VIII. as medidas de contenção, mitigação adotadas e sua efetividade.

A caracterização do risco ou dano relevante poderá ocorrer, dentre outras hipóteses, quando o incidente:

I. puder impedir o exercício de direitos pelos titulares;
II. puder ocasionar danos materiais, morais, reputacionais ou discriminatórios;
III. envolver risco de fraude, uso indevido de identidade ou comprometimento da segurança dos titulares.

A avaliação deverá considerar, ainda, a ocorrência de pelo menos uma das seguintes circunstâncias:

I. envolvimento de dados pessoais sensíveis;
II. envolvimento de dados de crianças, de adolescentes ou de idosos;
III. envolvimento de dados financeiros;
IV. envolvimento de dados de autenticação em sistemas;
V. envolvimento de dados protegidos por sigilo legal, judicial ou profissional; ou
VI. tratamento de dados em larga escala.

A avaliação deverá ser suficiente para subsidiar a decisão quanto à comunicação, ainda que realizada com base em informações preliminares.

Nem todo incidente de segurança da informação caracteriza incidente envolvendo dados pessoais sujeito à comunicação prevista na Lei nº 13.709/2018 e na Resolução CD/ANPD nº 15/2024.

A mera existência de vulnerabilidade em sistema, serviço ou infraestrutura tecnológica, sem evidência de comprometimento das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais, não caracteriza, por si só, incidente sujeito à comunicação.

A decisão quanto à necessidade de comunicação deverá ser fundamentada e registrada no processo administrativo correspondente.

4.1 DO RECEBIMENTO DA NOTIFICAÇÃO SOBRE O INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

O Encarregado pelo tratamento de dados pessoais atua como canal institucional de comunicação e coordenação das medidas relacionadas aos incidentes envolvendo dados pessoais no âmbito da UFOB, com atuação integrada da ETIR-UFOB, do gestor da base de dados afetada e das demais unidades envolvidas, quando pertinente.

O incidente poderá ser identificado ou comunicado por qualquer agente interno ou externo à universidade, mediante utilização dos canais institucionais disponíveis, inclusive mensagem eletrônica, comunicação da Ouvidoria, chamado técnico, atendimento presencial, ligação telefônica ou outro meio apto a permitir a ciência do fato pela UFOB.

Para os agentes internos da universidade, a notificação deverá ser realizada, preferencialmente, mediante abertura de processo eletrônico no SIPAC, do tipo "Gestão da Informação: incidente de segurança", contendo o Formulário de Notificação de Incidente de Segurança constante do **Anexo I**, bem como os documentos e evidências disponíveis relacionados ao incidente.

O processo deverá ser encaminhado ao Encarregado pelo tratamento de dados pessoais para coordenação das medidas de análise, contenção, mitigação, registro e comunicação do incidente.

A ausência de formalização imediata do processo administrativo não impede a adoção das medidas necessárias de análise, contenção, mitigação ou comunicação do incidente.

Para usuários externos à universidade, a comunicação do incidente poderá ser realizada por meio da plataforma Fala.BR, inclusive de forma anônima, sem prejuízo da utilização de outros canais institucionais disponíveis.

4.2 DA ANÁLISE DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

A análise do incidente de segurança envolvendo dados pessoais deverá ser realizada de forma prioritária e tempestiva, com a finalidade de subsidiar:

I. a caracterização do incidente;
II. a avaliação quanto à existência de risco ou dano relevante aos titulares; e
III. a decisão quanto à necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

A análise será realizada de forma integrada pelo Encarregado, pela ETIR-UFOB, pelo gestor da base de dados afetada e pelas demais unidades envolvidas, quando pertinente, observadas as competências previstas neste documento.

Compete ao Encarregado decidir quanto:

I. à caracterização do incidente envolvendo dados pessoais;
II. à existência de risco ou dano relevante aos titulares; e
III. à necessidade de comunicação do incidente.

A decisão deverá ser fundamentada e registrada no processo administrativo correspondente.

O Relatório de Tratamento do Incidente (RTI) constitui instrumento de registro técnico e administrativo do incidente, destinado à documentação:

I. das circunstâncias do incidente;
II. das análises realizadas;
III. das medidas adotadas;
IV. das decisões relacionadas ao tratamento e à comunicação do incidente.

O RTI deverá integrar o processo administrativo correspondente e conter, sempre que disponíveis:

I. identificação do incidente, incluindo datas de ocorrência, detecção e ciência pelo controlador;
II. descrição do incidente e das circunstâncias relacionadas;
III. identificação dos sistemas, serviços ou bases de dados afetadas;
IV. natureza, categoria e volume estimado dos dados pessoais afetados;
V. número estimado de titulares afetados;
VI. avaliação dos riscos e dos possíveis impactos aos titulares;
VII. medidas de contenção, mitigação e correção adotadas;
VIII. informações sobre eventual comunicação à ANPD e aos titulares;
IX. identificação das unidades e agentes envolvidos;
X. registros e evidências relacionados ao incidente.

As informações previstas nesta Subseção deverão ser registradas conforme o modelo constante do **Anexo II**.

Quando o incidente envolver atividades de tratamento que possam gerar alto risco às liberdades civis e aos direitos fundamentais dos titulares, poderá ser utilizado, de forma complementar, o Relatório de Impacto à Proteção de Dados Pessoais, sem prejuízo da elaboração do Relatório de Tratamento do Incidente.

5. DA COMUNICAÇÃO DO INCIDENTE À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Verificada a necessidade de comunicação, o Encarregado deverá comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) no prazo de três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.

A comunicação constitui ato do controlador, realizado por intermédio do Encarregado, mediante utilização do canal eletrônico disponibilizado pela ANPD para essa finalidade, conforme orientações disponíveis em seu sítio eletrônico oficial.

O ato de comunicação deverá ser acompanhado de documento comprobatório do vínculo funcional do Encarregado, nos termos do § 5º do art. 6º da Resolução CD/ANPD nº 15/2024.

A comunicação deverá conter, sempre que disponíveis, as seguintes informações:

I. a descrição da natureza e da categoria de dados pessoais afetados;
II. o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
III. as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
IV. os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;
V. os motivos da demora, no caso de a comunicação não ter sido realizada no prazo;
VI. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente;

VII. a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

VIII. os dados do encarregado ou de quem represente o controlador;

IX. a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

X. a identificação do operador, quando aplicável;

XI. a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la;

XII. o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

A ausência de informações completas no momento da comunicação não impede sua realização no prazo legal, devendo as informações supervenientes ser complementadas posteriormente, nos termos da Resolução CD/ANPD nº 15/2024.

Nos casos que envolvam informações protegidas por sigilo legal, judicial ou profissional, o Encarregado poderá solicitar à ANPD, de forma fundamentada, a restrição de acesso às informações cuja divulgação possa representar violação ao sigilo aplicável.

As informações relacionadas à comunicação do incidente deverão ser registradas no processo administrativo correspondente.

6. DA COMUNICAÇÃO DO INCIDENTE AOS TITULARES

Verificada a necessidade de comunicação aos titulares, o Encarregado deverá comunicar o incidente no prazo de três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. A comunicação deverá conter, sempre que disponíveis, as seguintes informações:

I. a descrição da natureza e da categoria de dados pessoais afetados;
II. as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os sigilos aplicáveis;
III. os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;
IV. os motivos da demora, caso a comunicação não tenha sido realizada no prazo;
V. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
VI. a data do conhecimento do incidente de segurança;
VII. o contato para obtenção de informações e, quando aplicável, os dados de contato do Encarregado.

A comunicação deverá ser realizada, preferencialmente, de forma direta e individualizada, mediante utilização dos meios usualmente empregados pela UFOB para contato com os titulares, tais como telefone, e-mail, mensagem eletrônica ou outros canais institucionais disponíveis.

Quando a comunicação direta e individualizada se mostrar inviável ou não for possível identificar, parcial ou integralmente, os titulares afetados, a comunicação poderá ser realizada de forma ampla, mediante divulgação nos canais institucionais

disponíveis, de modo a permitir o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de três meses.

Nas hipóteses de comunicação ampla, a Diretoria de Comunicação Institucional e Científica (DIRCOM) prestará apoio à divulgação institucional, em articulação com o Encarregado.

As informações relacionadas à comunicação do incidente aos titulares deverão ser registradas no processo administrativo correspondente.

7. DO REGISTRO E DA RASTREABILIDADE DO INCIDENTE

A UFOB deverá manter registro dos incidentes de segurança envolvendo dados pessoais, inclusive daqueles em que não houver comunicação à Autoridade Nacional de Proteção de Dados (ANPD) ou aos titulares, observadas as normas aplicáveis de gestão documental e preservação da informação.

O registro do incidente deverá assegurar a rastreabilidade das medidas adotadas, das análises realizadas e das decisões relacionadas ao tratamento e à comunicação do incidente, em observância ao princípio da responsabilização e prestação de contas (*accountability*).

A decisão quanto à realização ou não da comunicação do incidente deverá ser fundamentada e registrada no processo administrativo correspondente.

Os registros e documentos relacionados ao incidente deverão permanecer vinculados ao processo administrativo correspondente.

8. PAPÉIS E RESPONSABILIDADES

Quadro 1: Papéis e responsabilidades

PAPEL	RESPONSABILIDADE
Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR-UFOB)	Identificar, registrar e realizar análise técnica preliminar do incidente; adotar medidas de contenção, mitigação e recuperação; preservar evidências; atuar de forma integrada com as unidades envolvidas.
Gestor da base de dados afetada	Prestar informações sobre os dados pessoais envolvidos, finalidade do tratamento, abrangência dos titulares afetados e impactos institucionais decorrentes do incidente.
Encarregado pelo tratamento de dados pessoais	Coordenar o fluxo institucional de análise e resposta ao incidente; avaliar a caracterização do incidente e a existência de risco ou dano relevante; decidir quanto à necessidade de comunicação; realizar as comunicações à ANPD e aos titulares.
DIRCOM	Apoiar a divulgação institucional da comunicação aos titulares, quando necessária comunicação ampla.
Reitor(a)	Ser cientificado(a) acerca da ocorrência de incidentes de segurança envolvendo dados pessoais e das medidas adotadas no âmbito da resposta institucional.

Fonte: Elaboração própria

9. DISPOSIÇÕES FINAIS

As disposições previstas neste manual deverão ser observadas pelas unidades da UFOB envolvidas no tratamento, resposta, análise, registro e comunicação de incidentes de segurança envolvendo dados pessoais.

Os casos omissos e as situações supervenientes relacionadas à aplicação deste manual serão analisados conforme as competências institucionais previstas na Política de Segurança da Informação da UFOB, na Lei nº 13.709/2018 e nas normas complementares da Autoridade Nacional de Proteção de Dados (ANPD).

O presente manual poderá ser revisado sempre que necessário, em razão de alterações normativas, aperfeiçoamentos institucionais ou atualização dos procedimentos relacionados à proteção de dados pessoais e à segurança da informação.

10. REFERÊNCIAS

BRASIL. **Lei nº 13.709**, **de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: Brasília, DF, 25 abr. 2024.

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA (UFOB). **Resolução CGAG/CONSUNI/UFOB nº 018/2023**. Institui a Política de Segurança da Informação da UFOB. Barreiras, BA: UFOB, 2023.

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA (UFOB). **Portaria UFOB nº 220, de 15 de março de 2021**. Institui o Comitê de Implementação da Lei Geral de Proteção de Dados na UFOB. Barreiras, BA: UFOB, 2021.

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA (UFOB). **Portaria PROTIC/UFOB nº 02, de 25 de julho de 2024**. Regulamenta a Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR-UFOB). Barreiras, BA: UFOB, 2024.

BRASIL. Tribunal de Contas da União (TCU). **Acórdão nº 1372/2025 – Plenário**. Auditoria de conformidade realizada pelo Tribunal de Contas da União (TCU) com o objetivo de diagnosticar os controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: TCU, 2025.

ANEXO I

Formulário de Notificação de Incidente de Segurança

Formulário de Notificação de Incidente de Segurança

Processo nº 23520.XXXXXX/XXXX-XX

IDENTIFICAÇÃO DO COMUNICANTE

Nome completo:

Unidade/Lotação:

E-mail de contato:

Telefone para contato:

Data da comunicação:

IDENTIFICAÇÃO PRELIMINAR DO INCIDENTE

Data e hora da ocorrência (quando conhecida):

Data e hora da identificação do incidente:

Descrição preliminar do incidente:

Descreva objetivamente o fato ocorrido, a forma de identificação do incidente, os sistemas, serviços ou meios envolvidos e, quando possível, a localização física ou lógica dos dados afetados.

Causa principal (quando identificada):

Sistema, serviço ou base de dados afetada:

DADOS PESSOAIS POTENCIALMENTE AFETADOS

Natureza dos dados pessoais:

( ) Dados pessoais gerais

( ) Dados pessoais sensíveis

Categoria dos dados envolvidos:

( ) Dados de crianças, adolescentes ou idosos

( ) Dados financeiros

( ) Dados de autenticação em sistemas

( ) Dados protegidos por sigilo legal, judicial ou profissional

( ) Dados em larga escala

Número estimado de titulares afetados:

CLASSIFICAÇÃO PRELIMINAR DO INCIDENTE

Tipo preliminar do incidente:

( ) Acesso não autorizado

( ) Divulgação indevida

( ) Alteração indevida

( ) Perda ou destruição de dados

( ) Indisponibilidade de sistemas ou dados

( ) Sequestro de dados (ransomware)

( ) Roubo ou furto de equipamento

( ) Outro: _____

Classificação preliminar administrativa:

( ) Baixo impacto

( ) Médio impacto

( ) Alto impacto

( ) Em análise

MEDIDAS INICIAIS ADOTADAS

Medidas preliminares de contenção, mitigação ou recuperação:

DOCUMENTOS E EVIDÊNCIAS DISPONÍVEIS

( ) Logs

( ) Capturas de tela

( ) Relatórios técnicos

( ) Mensagens eletrônicas

( ) Outros: _____

Observações adicionais:

ANEXO II

Relatório de Tratamento de Incidente (RTI)

Relatório de Tratamento do Incidente (RTI)

Processo nº 23520.XXXXXX/XXXX-XX

O presente relatório destina-se ao registro do incidente de segurança da informação com dados pessoais, nos termos do art. 10 da Resolução CD/ANPD nº 15/2024, contemplando, no mínimo, as informações obrigatórias relativas ao registro do incidente, sem prejuízo da inclusão de outras informações necessárias à adequada análise, tratamento e comunicação.

IDENTIFICAÇÃO DO INCIDENTE

Data da ocorrência (quando conhecida):

Data da detecção:

Data da ciência pelo controlador:

Descrição geral do incidente:

Causa principal (quando identificada):

Outras informações relevantes:

SISTEMAS, SERVIÇOS E BASES AFETADAS

Identificação dos sistemas, serviços ou bases de dados afetadas:

DADOS PESSOAIS AFETADOS

Natureza dos dados:

( ) Dados pessoais gerais

( ) Dados pessoais sensíveis

Categoria dos dados:

( ) Dados de crianças, adolescentes ou idosos

( ) Dados financeiros

( ) Dados de autenticação em sistemas

( ) Dados protegidos por sigilo legal, judicial ou profissional

( ) Dados em larga escala

Volume estimado de dados afetados:

Número estimado de titulares afetados:

AVALIAÇÃO DE RISCO E IMPACTO

Avaliação dos riscos identificados:

Possíveis impactos aos titulares:

Caracterização de risco ou dano relevante:

( ) Sim

( ) Não

Fundamentação da avaliação:

MEDIDAS ADOTADAS

Medidas de contenção:

Medidas de mitigação:

Medidas corretivas:

Situação atual do incidente:

( ) Em análise

( ) Contido

( ) Mitigado

( ) Encerrado

DECISÃO QUANTO À COMUNICAÇÃO

Comunicação à ANPD:

( ) Sim

( ) Não

Comunicação aos titulares:

( ) Sim

( ) Não

Fundamentação da decisão:

Justificativa da ausência de comunicação (quando aplicável):

Responsável pela decisão:

COMUNICAÇÕES REALIZADAS

Data da comunicação à ANPD:

Síntese das informações prestadas:

Forma de comunicação aos titulares:

( ) Individual

( ) Comunicação ampla

Meios utilizados:

Data da comunicação aos titulares:

RESPONSÁVEIS ENVOLVIDOS

ETIR-UFOB:

Gestor da base de dados afetada:

Encarregado pelo tratamento de dados pessoais:

Outras unidades envolvidas:

EVIDÊNCIAS E DOCUMENTOS

Documentos e evidências relacionados ao incidente:

Descrição: