SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
COMITÊ DE GOVERNANÇA RISCOS E CONTROLES
Rodovia SC 484 - km 02, Fronteira Sul, Chapecó-SC, CEP 89815-181, 49 2049-3700
gabinete@uffs.edu.br, www.uffs.edu.br

RESOLUÇÃO Nº 06/CGRC/UFFS/2026

Aprova o Guia de Comunicação de Incidentes de Segurança da Informação com Dados Pessoais da Universidade Federal da Fronteira Sul

O PRESIDENTE DO COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES (CGRC) DA UNIVERSIDADE FEDERAL DA FRONTEIRA SUL (UFFS), no uso de suas atribuições legais, considerando:

A. as deliberações da 1ª Sessão Ordinária de 2026.

RESOLVE

Art 1º Aprovar o Guia de Comunicação de Incidentes de Segurança da Informação com Dados Pessoais da Universidade Federal da Fronteira Sul, conforme documento em anexo.

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

Sala de Reuniões da Reitoria em Chapecó-SC, 6 de maio de 2026.

João Alfredo Braida
Presidente do Comitê de Governança, Riscos e Controles

ANEXO I

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

GUIA DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

MAIO/2026

GUIA DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS – UFFS

1. OBJETIVO E FUNDAMENTAÇÃO LEGAL

Este documento estabelece o modelo institucional de comunicação de incidentes de segurança da informação que envolvam dados pessoais na Universidade Federal da Fronteira Sul (UFFS), em conformidade com:

- **Lei nº 13.709/2018 (LGPD)**, Art. 48, caput;
- **Resolução CD/ANPD nº 15/2024**, que regulamenta a Comunicação de Incidente de Segurança;
- **Acórdão TCU nº 1.372/2025-TCU-Plenário**, item 9.2.4, que determina a elaboração e aplicação do modelo em 180 dias – "adotem ações para elaborarem e aplicarem modelo de comunicação à ANPD e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, conforme disposto na Lei 13.709/2018, art. 48, *caput"*.
- Diretrizes de Governança Digital e Proteção de Dados no âmbito do Governo Federal.

O guia visa padronizar a notificação, análise, comunicação e registro de incidentes, garantindo transparência, mitigação de riscos e conformidade legal na Universidade Federal da Fronteira Sul.

2. ESCOPO E DEFINIÇÕES

Escopo: Aplica-se a todas as instâncias administrativas e acadêmicas da que fazem parte da Universidade Federal da Fronteira Sul e que realizem tratamento de dados pessoais em nome da UFFS.

Definições essenciais (conforme LGPD e Res. ANPD 15/2024):

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Agente de tratamento de dados:** Controlador e operador.
- **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD)

- **Incidente de Segurança:** Evento adverso confirmado que comprometa confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.
- **Dado Pessoal Afetado:** Aquele cuja segurança foi violada.
- **Titular:** Pessoa natural a quem se referem os dados.
- **Comunicação de incidente de segurança:** ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares

3. CARACTERIZAÇÃO DO INCIDENTE E CRITÉRIOS DE RISCO RELEVANTE

A comunicação é obrigatória quando o incidente **puder afetar significativamente interesses e direitos fundamentais** e, cumulativamente, envolver pelo menos um dos critérios:

1. Dados pessoais sensíveis;
2. Dados de crianças, adolescentes ou idosos;
3. Dados financeiros;
4. Dados de autenticação em sistemas;
5. Dados protegidos por sigilo legal, judicial ou profissional;
6. Dados em larga escala (número significativo de titulares, volume, duração, frequência ou extensão geográfica).

Alguns exemplos aplicáveis à UFFS: exposição de históricos acadêmicos ou médicos, comprometimento de credenciais de servidores/discentes, vazamento de folha de pagamento, fraude em processos seletivos, ransomware em sistemas de RH ou acadêmicos.

4. FLUXO OPERACIONAL: RECEBIMENTO, ANÁLISE E DECISÃO

Etapa	Responsável	Prazo	Ação
4.1 Recebimento	Interessado	Imediato	1. O incidente deverá ser registrado, preferencialmente, via Plataforma Fala.BR(https://falabr.cgu.gov.br/), como “Solicitação de Providências”. 2. O manifestante deverá preencher o formulário de Notificação de Incidente – UFFS (Anexo I) e anexá-lo à manifestação. 3. Além do Formulário, poderão ser anexados outros documentos que comprovem e caracterizem o incidente de segurança. 4. A Ouvidoria da UFFS remeterá a manifestação ao Encarregado via Plataforma Fala.Br. 5. O Encarregado instruirá processo no SIPAC para tratar a manifestação. 6. Caso não haja informações suficientes para a caracterização completa do incidente de segurança, o encarregado poderá solicitar informações complementares à pessoa manifestante. 7. Caso a manifestação ocorra de forma anônima, o demandante deverá fazer o registro o mais completo possível, pois não será possível solicitar complementação. 8. Encarregado preencherá o Formulário constante no Anexo II e colocará como peça do processo no SIPAC.
4.2 Triagem e Análise	Encarregado + Área afetada	Até 3 dias úteis	1. O encarregado responsável analisará a manifestação e identificará a natureza e a categoria dos dados pessoais afetados, o volume/número de titulares afetados, os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares, no prazo de 3 (três) dias úteis, conforme Resolução CD/ANPD Nº 15/2024. 2. Sendo necessário, o encarregado poderá solicitar colaboração de setores institucionais que atuam com os referidos dados pessoais, encaminhando o processo no SIPAC, e estes atuarão na complementação da análise, de forma a subsidiar a confirmação ou não do incidente de segurança, sua extensão, a natureza dos dados afetados e riscos diversos. 3. Após análise e complementação de informações, o setor deverá restituir o processo no SIPAC ao encarregado, dentro do prazo mencionado no Despacho do encarregado.

			4. O encarregado adotará medidas técnicas e administrativas necessárias à contenção, mitigação e tratamento de insegurança que serão registradas no processo administrativo.
4.3 Decisão	Encarregado	Até 3 dias úteis	1. Confirmando-se que se trata de incidente de segurança com dados pessoais, o encarregado, deverá proceder imediatamente à comunicação à Agência Nacional de Proteção de Dados (ANPD) e ao titular dos dados, conforme instrui este guia.
		Após a conclusão da análise	2. Comunicar formalmente à Ouvidoria, via Plataforma Fala.Br, o resultado consolidado da análise do incidente, para fins de registro institucional e encerramento da manifestação.
		Quando aplicável	3. Verificada a existência de indícios de irregularidade administrativa, disciplinar ou ilícito relacionado ao incidente, ***promover comunicação específica à Ouvidoria***, mediante novo registro no Fala.Br ***(Denúncia)***, contendo relato sucinto dos fatos e apenas os documentos estritamente necessários a subsidiar eventual apuração.

5. COMUNICAÇÃO À AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Responsável pela comunicação: O encarregado de dados da UFFS

Meio: Formulário eletrônico oficial da ANPD (https://www.gov.br/anpd). O encarregado deverá seguir os procedimentos indicados no site da ANPD - Comunicação de Incidente de Segurança - https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Após acessar o SEI (usuário externo), deverá peticionar "novo processo" e preencher o Formulário "SFI: Comunicados de Incidentes à Agência Nacional de Proteção de Dados".

Prazo: Até **3 dias úteis** após o conhecimento confirmado do incidente e que este tenha afetado dados pessoais.

Conteúdo obrigatório constante na comunicação (Art. 6º, §2º, Res. 15/2024):

1. Natureza e categoria dos dados afetados;
2. Número de titulares afetados (discriminando crianças/adolescentes/idosos, se aplicável);
3. Medidas técnicas/administrativas de proteção (antes e depois);
4. Riscos e possíveis impactos aos titulares;
5. Motivos de eventual atraso na comunicação;
6. Medidas adotadas ou planejadas para reverter/mitigar efeitos;
7. Data da ocorrência e data do conhecimento pelo controlador;
8. Dados do Encarregado ou representante legal;
9. Identificação do controlador (e declaração de porte, se aplicável);
10. Identificação do operador (se houver);
11. Descrição do incidente e causa principal (se identificada);
12. Total de titulares cujos dados são tratados nas atividades afetadas.

Observações: Complementações fundamentadas podem ser enviadas em até **20 dias úteis**. De acordo com o Art. 8º da Resolução CD/ANPD Nº 15/2024, a ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

6. COMUNICAÇÃO AOS TITULARES DOS DADOS

Prazo: Até **3 dias úteis** contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.

Meio e Formato:

- **Preferencial:** Direta e individualizada (e-mail institucional, carta, telefone, SMS, whatsApp).
- **Alternativa:** Canais institucionais (site UFFS, intranet, murais digitais, redes sociais oficiais) por, no mínimo, **3 meses**, quando a identificação direta for inviável.
- **Linguagem:** Clara, acessível, sem termos excessivamente técnicos.

Conteúdo obrigatório (Art. 9º, Res. 15/2024):

1. Natureza e categoria dos dados afetados;
2. Medidas de segurança adotadas;
3. Riscos e possíveis impactos;
4. Motivos de eventual atraso;
5. Medidas de reversão ou mitigação;
6. Data do conhecimento do incidente;
7. Contato para informações (incluindo DPO).

Boa prática: Incluir recomendações práticas ao titular (ex.: alteração de senhas, monitoramento de contas, canal de suporte) conforme Art. 52, §1º, IX, LGPD.

Ainda, em observância ao disposto no Art. 9º da Resolução CD/ANPD Nº 15/2024, o Encarregado providenciará a inclusão, na comunicação ao titular, de recomendações aptas a reverter ou mitigar os efeitos do incidente, considerada como boa prática, à luz do disposto no Art. 52, § 1º, Inciso IX, da LGPD.

7. REGISTRO, RETENÇÃO E GOVERNANÇA

A UFFS manterá registro interno de **todos** os incidentes (comunicados ou não), por **5 anos** a partir da data de registro, salvo obrigação legal diversa.

Conteúdo mínimo do registro (Art. 10, §2º, Res. 15/2024):

1. Data de conhecimento;
2. Circunstâncias gerais;
3. Natureza e categoria dos dados;
4. Número de titulares;
5. Avaliação de risco e possíveis danos;

6. Medidas corretivas/mitigadoras;
7. Forma e conteúdo da comunicação (se realizada);
8. Motivo da ausência de comunicação (se aplicável).

Armazenamento: Processo digital no SIPAC UFFS ou outro repositório seguro com acesso restrito. Revisão anual pelo Comitê de Governança Digital.

8. REFERÊNCIAS

1. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
2. ANPD. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Regulamento de Comunicação de Incidente de Segurança.
3. TCU. Acórdão nº 1.372/2025-TCU-Plenário. Determinações sobre implementação de modelo de comunicação de incidentes.
4. UFFS. Normativos internos de Governança Digital, Segurança da Informação e Processo Administrativo Digital.

ANEXO I – FORMULÁRIO DE NOTIFICAÇÃO DE INCIDENTE - UFFS

Campo	Informação
Nome / Lotação / Contato	
Data/Hora da Ocorrência (ou suspeita)	
Descrição Objetiva	(O que ocorreu, como foi descoberto, sistemas/meios envolvidos, localização física/lógica)
Causa Principal (se conhecida)	
Natureza dos Dados	☐ Gerais ☐ Sensíveis (especificar: origem racial, religiosa, política, saúde, vida sexual, biométrico, genético)
Categoria dos Dados	☐ Crianças/Adolescentes/Idosos ☐ Financeiros ☐ Autenticação ☐ Sigilo Legal/Judicial/Profissional ☐ Larga Escala
Nº Estimado de Titulares	
Tipo de Violação Suspeito	☐ Acesso não autorizado ☐ Vazamento ☐ Alteração ☐ Perda/Destruição ☐ Ransomware ☐ Roubo/Furto ☐ Outro:
Documentos Anexados	(logs, prints, relatórios técnicos, etc.)

ANEXO II – FORMULÁRIO DE REGISTRO DE INCIDENTE PELO Encarregado/UFFS

(Preenchimento interno após análise – armazenar em processo SIPAC)

Campo	Informação
Data de Conhecimento	
Circunstâncias Gerais	
Natureza/Categoria dos Dados	
Nº de Titulares Afetados	
Avaliação de Risco / Possíveis Danos	
Medidas Corretivas	
Medidas Mitigadoras	
Comunicação à ANPD	☐ Sim ☐ Não – Justificativa:
Comunicação aos Titulares	☐ Sim ☐ Não – Meio utilizado:
Observações / Anexos	