



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
COMITÊ DE GOVERNANÇA DIGITAL

Norma Operacional CGD/UFERSA nº 01/2026

Mossoró/RN, 06 de Janeiro de 2026

Normatiza os procedimentos internos para comunicar à Agência Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança, no âmbito da Universidade Federal Rural do Semi-árido – UFERSA.

O Presidente do Comitê Governança Digital da Universidade Federal Rural do Semi-Árido (UFERSA), no uso de suas atribuições legais e com base na deliberação deste Órgão Colegiado em Reunião Extraordinária realizada em 22 de dezembro de 2025, e considerando:

- I. o disposto na Lei nº 13.709, de 14 de agosto de 2018
- II. a resolução CD/ANPD Nº 15, de 24 de abril de 2024
- III. A Política de Segurança da Informação da UFERSA – POSIC, regulamentada pela Resolução Consuni 015/2017, de 15 de dezembro de 2017;

Resolve:

Art 1º Estabelecer os procedimentos para comunicar à Agência Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança, no âmbito da Universidade Federal Rural do Semi-árido – UFERSA

Art. 2º Para fins desta Norma Operacional (NO), entende-se por:

- I **Incidente de segurança com dados pessoais:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais;
- II **ANPD:** Agência Nacional de Proteção de Dados Pessoais, encarregada por zelar pela proteção dos dados pessoais, nos termos da legislação;
- III **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);
- IV **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- V **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
COMITÊ DE GOVERNANÇA DIGITAL

- VI **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- VII **Descoberta de um incidente:** momento em que a instituição toma conhecimento de um incidente por seus próprios meios ou informada por terceiros;

Art. 3º A comunicação de incidente de segurança com dados pessoais inicia-se com a descoberta do incidente que pode ocorrer:

- I Por ação de servidor ou setor da Instituição que identifica a ocorrência e informa à Superintendência de Tecnologia da informação e comunicação, ao encarregado ou ao Comitê de Governança digital;
- II Por ação da Superintendência de Tecnologia da informação e comunicação;
- III Por informação/denúncia por um dos canais oficiais da instituição;
- IV Por divulgação em mídia ou rede social;

Art. 4º Feita a descoberta, a Equipe de tratamento de Incidentes de Segurança deve ser acionada e iniciar imediatamente as etapas de (a) Isolamento e Contenção, (b) Identificação e Classificação, (c) Investigação, (d) Recuperação de Dados e serviços (caso seja necessário) e (e) Notificação à Reitoria, ao Comitê de Governança Digital e ao Encarregado e, construção de Relatórios.

Parágrafo Único: O registro do incidente deve conter pelo menos:

- I a data de conhecimento do incidente;
- II a descrição geral das circunstâncias em que o incidente ocorreu;
- III a natureza e a categoria de dados afetados;
- IV o número de titulares afetados;
- V a avaliação do risco e os possíveis danos aos titulares;
- VI as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- VII a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
- VIII os motivos da ausência de comunicação, quando for o caso.

Art. 5º A comunicação de incidente de segurança com dados pessoais observará as seguintes etapas:

- I Avaliar incidente internamente: serão avaliadas a natureza, a categoria e a quantidade de titulares de dados afetados, a categoria e quantidade dos dados afetados, as consequências concretas e prováveis, atividade que será conduzida pela área diretamente envolvida no incidente, independente do meio utilizado para armazenamento dos dados;



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
COMITÊ DE GOVERNANÇA DIGITAL

- II Comunicar ao Encarregado: comunicar formalmente a ocorrência do incidente ao Encarregado pelo Tratamento de Dados Pessoais da instituição;
- III Comunicar ao Controlador: o Controlador será comunicado formalmente a respeito da ocorrência do incidente;
- IV Comunicar à ANPD e ao(s) titular(es) de dados: caso o incidente envolva risco ou dano relevante aos titulares, comunicar formalmente à ANPD e ao(s) titular(es) de dados envolvidos;
- V Elaborar documentação: realizar registro formal onde conste a avaliação interna do incidente com os dados de identificação dos responsáveis por sua elaboração, as medidas de contorno empregadas, a análise de risco, as medidas empregadas para preservação das evidências, para fins de cumprimento do princípio de responsabilização e prestação de contas.

Art. 6º A comunicação de incidente de segurança com dados pessoais será realizada exclusivamente pelo Encarregado de Dados da UFERSA, em ação coordenada com o Gabinete da Reitoria.

Parágrafo 1º - Essa comunicação será feita em até 3 dias úteis após a tomada de conhecimento pelo controlador.

Parágrafo 2º - Caso a investigação citado no artigo 3º não tenha sido encerrada no prazo de 3 dias úteis, informações complementares poderão ser encaminhadas posteriormente à ANPD.

Art. 7º O conteúdo da comunicação enviado à ANPD conterá, no mínimo, 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 comerciais e industriais;
- 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 previsto no artigo 6º;
- VI Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- 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;



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
COMITÊ DE GOVERNANÇA DIGITAL

- 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; e
- XII O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Art. 8º O conteúdo da comunicação enviado ao(s) titular(es) deverá conter, no mínimo, 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 segredos comerciais e industriais;
- III Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- IV Os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;
- 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; e
- VII O contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

Parágrafo 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

- I Fazer uso de linguagem simples e de fácil entendimento; e
- II Ocorrer de forma direta e individualizada, caso seja possível identificá-los.

Parágrafo 2º Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

Parágrafo 3º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, preferencialmente pelo portal institucional e mídias sociais da Instituição.

Art. 9º A decisão sobre realizar ou não a comunicação de incidente de segurança com dados pessoais será pautada pelos seguintes princípios:



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
COMITÊ DE GOVERNANÇA DIGITAL

- I O incidente de segurança pode acarretar um risco ou dano relevante aos titulares afetados, a impossibilidade do exercício de um direito fundamental, acesso a um serviço essencial, discriminação, perda de reputação ou o uso indevido de imagem;
- II Sempre que o incidente tiver sido divulgado publicamente;
- III Sempre que o incidente envolver dados compartilhados com outras instituições de ensino, órgãos públicos ou similares;
- IV Sempre que envolver:
 - a. Dados pessoais sensíveis;
 - b. Dados de crianças, de adolescentes ou de idosos;
 - c. Dados financeiros;
 - d. Dados de autenticação em sistemas;
 - e. Dados protegidos por sigilo legal, judicial ou profissional; ou
 - f. Dados em larga escala (grande número de titulares).
- V Atender a critérios complementares definidos pela ANPD.

Art. 10 Em caso de qualquer tipo de omissão ou negligência por parte dos envolvidos, cabe ao Controlador aplicar as medidas disciplinares cabíveis previstas na legislação vigente.

Art. 11. O processo de comunicação de incidente de segurança será declarado extinto nas seguintes hipóteses:

- I Caso não sejam identificadas evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;
- II Uma vez feita comunicação à ANPD, esta considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares;
- III Caso o incidente não envolva dados pessoais;
- IV Caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou
- V Realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD, as disposições deste Regulamento e as determinações da ANPD.

Art. 12 Os casos omissos neste documento serão analisados e resolvidos pelo Controlador, com apoio do Operador.

Art. 13 Esta Norma operacional entra em vigor no ato de sua publicação.

Nildo da Silva Dias
Presidente do CGD