Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

INOR Nº2/2026/COI/IFSULDEMINAS

INSTRUÇÃO NORMATIVA

Institui o Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais no âmbito do IFSULDEMINAS.

Art. 1º Fica estabelecido o Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – IFSULDEMINAS, constante do Anexo I desta Instrução Normativa.

Art. 2º O Guia tem por finalidade estabelecer orientações, procedimentos e responsabilidades relacionados à identificação, registro, tratamento, resposta e comunicação de incidentes de segurança da informação que envolvam dados pessoais tratados pelo IFSULDEMINAS, observadas as disposições da Lei nº 13.709, de 14 de agosto de 2018, da Resolução CD/ANPD nº 15, de 24 de abril de 2024, da Política de Privacidade e Proteção de Dados Pessoais do IFSULDEMINAS e da Política de Segurança da Informação da instituição.

Art. 3º O Guia instituído por esta Instrução Normativa aplica-se a todas as unidades do IFSULDEMINAS e deverá ser observado pelos agentes públicos, estudantes, colaboradores, prestadores de serviço e demais usuários que, de qualquer forma, participem de atividades relacionadas ao tratamento de dados pessoais ou à comunicação de incidentes de segurança da informação no âmbito institucional.

Art. 4º As propostas de atualização do Guia serão coordenadas pela Coordenação de Integridade e Controle Interno - COI, com a participação do Encarregado pelo Tratamento de Dados Pessoais - DPO, da Coordenadoria de Segurança e Proteção de Dados Digitais - CSPD e da Diretoria de Tecnologia da Informação - DTI, sem prejuízo da manifestação de outras unidades competentes quando necessária.

Art. 5º Os casos omissos serão analisados pela Coordenação de Integridade e Controle Interno – COI, ouvidas as unidades competentes em razão da matéria.

Art. 6º Esta Instrução Normativa entra em vigor na data de sua publicação.

Documentos Anexados:

- **Anexo #1.** Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais no âmbito do IFSULDEMINAS. (anexado em 16/06/2026 09:37:01)

Documento assinado eletronicamente por:

- **Pamela Helia de Oliveira**, **COORDENADOR(A) GERAL - CD4 - IFSULDEMINAS - COI**, em 16/06/2026 09:37:32.

Este documento foi emitido pelo SUAP em 16/06/2026. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 673566
Código de Autenticação: ed4cd4dc8a

Nível de Acesso: Público
16/06/2026 09:36 - Criado inicialmente como: Público.

INSTITUTO FEDERAL
Sul de Minas Gerais

GUIA

DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS NO IFSULDEMINAS

IFSULDEMINAS . MAIO 2026

SUMÁRIO

Resumo Executivo

CONTROLADOR - INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SUL DE MINAS GERAIS

GUIA DE DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS NO IFSULDEMINAS

EQUIPE TÉCNICA DE ELABORAÇÃO

- **COORDENAÇÃO DE INTEGRIDADE E CONTROLE INTERNO – COI**
- **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO – DTI**
- **COORDENADORIA DE SEGURANÇA E PROTEÇÃO DE DADOS DIGITAIS – CSPD**
- **ENCARREGADO DE DADOS – DPO**

REVISÃO E APROVAÇÃO

- EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS – ETIR
- CONTROLADOR (IFSULDEMINAS) – AUTORIDADE MÁXIMA DESIGNADA

VERSÃO

1.0 JUNHO DE 2026

1. APRESENTAÇÃO

O Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais, no exercício de suas atribuições institucionais, em conformidade com a Política de Privacidade e Proteção de Dados Pessoais do IFSULDEMINAS, aprovada pela Resolução nº 131/2021/CONSUP, realiza continuamente operações de tratamento de dados pessoais necessárias à execução de políticas públicas educacionais, administrativas, científicas e de extensão, envolvendo informações de estudantes, servidores, colaboradores, fornecedores e demais cidadãos que se relacionam com a instituição.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais estabelece que os agentes de tratamento de dados pessoais — controladores e operadores — devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como medidas voltadas à prevenção de danos aos titulares decorrentes de suas atividades.

Em caso de incidente de segurança envolvendo dados pessoais, uma das principais medidas de mitigação consiste na comunicação tempestiva da ocorrência à Autoridade Nacional de Proteção de Dados e, quando aplicável, aos titulares dos dados afetados, possibilitando a adoção de providências destinadas à redução de riscos, à mitigação de impactos e à preservação dos direitos fundamentais de liberdade, privacidade e proteção de dados pessoais.

Tal obrigação decorre do art. 48 da Lei nº 13.709/2018, segundo o qual o controlador deverá comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A matéria foi regulamentada pela Autoridade Nacional de Proteção de Dados, que aprovou o Regulamento de Comunicação de Incidente de Segurança, estabelecendo critérios, procedimentos e parâmetros para avaliação da necessidade de comunicação.

No âmbito institucional, o presente **GUIA DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS NO IFSULDEMINAS** constitui instrumento de governança destinado a orientar o fluxo institucional de identificação, análise, registro, tratamento e comunicação de incidentes de segurança que envolvam dados pessoais, observando as disposições da Política de Privacidade e Proteção de Dados Pessoais do IFSULDEMINAS, aprovada pela Resolução nº 131/2021/CONSUP, da Política de Segurança da Informação do IFSULDEMINAS, aprovada pela Resolução nº 355/2023/CONSUP, bem como das demais diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

A atuação institucional diante de incidentes deverá observar a integração entre as áreas responsáveis pela governança, tecnologia da informação, segurança da informação, privacidade, comunicação institucional e gestão administrativa, com participação técnica da Diretoria de Tecnologia da Informação, do Encarregado pelo Tratamento de Dados Pessoais, das unidades administrativas envolvidas e das instâncias de governança competentes, conforme a natureza e a criticidade do evento ocorrido.

Cumpre destacar que nem todo incidente de segurança ensejará comunicação à Autoridade Nacional de Proteção de Dados ou aos titulares. Caberá à instituição, mediante análise técnica e jurídica do caso concreto, avaliar a probabilidade de risco ou dano relevante aos titulares, considerando a natureza dos dados afetados, o volume de registros envolvidos, a possibilidade de uso indevido, os impactos potenciais aos direitos dos titulares e as medidas de contenção já adotadas.

Dessa forma, o presente Guia objetiva fortalecer a maturidade institucional em privacidade e segurança da informação, estabelecer procedimentos padronizados para resposta a incidentes e promover atuação coordenada, tempestiva e transparente diante de eventos que possam comprometer a confidencialidade, integridade e disponibilidade de dados pessoais tratados pelo IFSULDEMINAS, reforçando o compromisso institucional com a proteção de dados, a integridade pública e a confiança da sociedade.

2. DISPOSIÇÕES ACERCA DO PROCESSO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD) e da regulamentação expedida pela Autoridade Nacional de Proteção de Dados (ANPD), os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais deverão ser formalmente analisados pela instituição, visando à identificação de sua gravidade, impactos e medidas de contenção, mitigação e tratamento.

No âmbito do IFSULDEMINAS, os incidentes de segurança poderão envolver ou não dados pessoais, devendo sua caracterização ocorrer a partir de análise técnica e administrativa conduzida pela ETIR-IFSULDEMINAS, pelo Encarregado pelo Tratamento de Dados Pessoais e pela unidade responsável pelas informações afetadas.

Quando identificado incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, a instituição deverá avaliar a necessidade de comunicação à ANPD e aos titulares afetados, observados os critérios legais e regulamentares aplicáveis.

A ANPD poderá, no exercício de sua competência fiscalizatória, requisitar informações, determinar medidas preventivas ou corretivas, realizar auditorias ou inspeções, bem como exigir providências destinadas à mitigação dos impactos decorrentes do incidente, nos termos da regulamentação vigente.

O descumprimento das medidas determinadas pela autoridade competente poderá ensejar responsabilização administrativa e eventual instauração de processo sancionador, sem prejuízo das demais medidas legais cabíveis.

3. CARACTERIZAÇÃO DE UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

Nos termos da Autoridade Nacional de Proteção de Dados, a ocorrência de incidente de segurança envolvendo dados pessoais deverá ser objeto de análise institucional quanto à necessidade de comunicação à Autoridade Nacional e, quando aplicável, aos titulares dos dados afetados, sempre que houver potencial de geração de risco ou dano relevante.

Considera-se que há risco ou dano relevante aos titulares quando o incidente puder impactar de maneira significativa direitos e liberdades fundamentais da pessoa natural, comprometer o exercício regular de direitos ou expor o titular a prejuízos materiais, morais ou reputacionais. Entre os possíveis impactos decorrentes de um incidente dessa natureza, destacam-se:

I – uso indevido de informações pessoais;
II – fraude, falsidade ideológica ou roubo de identidade;
III – exposição indevida da imagem, reputação ou vida privada do titular;
IV – discriminação ou tratamento desigual em razão de características pessoais;
V – prejuízo financeiro ou patrimonial;
VI – comprometimento da integridade física ou da segurança pessoal do titular;
VII – restrição ou inviabilização do acesso do titular a serviços, direitos ou benefícios.

A caracterização de incidente com potencial de risco ou dano relevante deverá considerar, cumulativamente, a existência de impacto significativo ao titular e o envolvimento de pelo menos uma das seguintes categorias de dados ou contextos de tratamento:
I – dados pessoais sensíveis;
II – dados pessoais de crianças, adolescentes ou idosos;
III – dados de natureza financeira;
IV – credenciais ou dados de autenticação utilizados para acesso a sistemas;
V – dados submetidos a sigilo legal, judicial ou profissional;
VI – elevado volume de dados pessoais ou de titulares potencialmente afetados pelo incidente.

Para fins deste Guia, considera-se incidente de segurança da informação com dados pessoais qualquer evento adverso confirmado que comprometa, ainda que potencialmente, a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais tratados institucionalmente.

Esses incidentes podem decorrer de falhas humanas, vulnerabilidades tecnológicas, fragilidades processuais ou ações maliciosas, podendo ocorrer, no contexto institucional do IFSULDEMINAS, em situações como:

I – envio indevido de informações pessoais
encaminhamento, por e-mail institucional, sistema eletrônico ou outro meio de comunicação, de documentos contendo dados pessoais a destinatário diverso do correto, como listas de estudantes, documentos funcionais, relatórios médicos ocupacionais, dados bancários ou informações acadêmicas.

II – divulgação não autorizada de dados pessoais
publicação acidental ou indevida, em portal institucional, sistema eletrônico, ambiente virtual de aprendizagem, mural público, grupo de mensagens ou outro canal de comunicação, de documentos ou informações contendo dados pessoais sem prévio consentimento, respaldo legal ou necessidade administrativa.

III – acesso indevido a sistemas institucionais
utilização não autorizada de credenciais, compartilhamento de login e senha, invasão de contas institucionais ou acesso indevido a sistemas como SUAP, ambientes acadêmicos, sistemas administrativos ou bases de dados institucionais.

IV – perda, furto ou extravio de dispositivos e documentos
desaparecimento, roubo ou descarte inadequado de computadores, notebooks, dispositivos móveis, mídias removíveis, documentos físicos ou arquivos digitais que contenham dados pessoais de estudantes, servidores, terceirizados ou demais titulares.

V – indisponibilidade de dados pessoais decorrente de comprometimento de serviços ou bases de dados interrupção parcial ou total de sistemas, serviços ou bases institucionais que impeça ou comprometa o acesso, a utilização ou a recuperação de dados pessoais tratados pelo IFSULDEMINAS.

VI – eliminação, alteração ou corrupção indevida de registros
apagamento acidental, modificação não autorizada ou comprometimento da integridade de históricos acadêmicos, assentamentos funcionais, prontuários administrativos, registros de frequência, cadastros institucionais ou outros dados pessoais sob guarda da instituição.

VII – comprometimento por software malicioso
ocorrência de ataque cibernético, criptografia indevida de arquivos (*ransomware*), instalação de programas maliciosos, captura de credenciais (*phishing*) ou outra ação que comprometa a segurança dos dados pessoais tratados pelo Instituto.

VIII – exposição inadequada em processos administrativos e documentos oficiais
compartilhamento excessivo de dados pessoais em processos eletrônicos, pareceres, publicações oficiais, atas, editais, portarias ou documentos administrativos, em desacordo com os princípios da necessidade, adequação e minimização previstos na LGPD.

IX – tratamento inadequado de dados pessoais sensíveis exposição, compartilhamento indevido ou armazenamento inseguro de informações relacionadas à saúde, biometria, inclusão, assistência estudantil, condições psicossociais, raça/cor, deficiência ou outras categorias especiais de dados pessoais.

X – incidentes envolvendo terceiros contratados falhas de segurança ocorridas em serviços terceirizados, fundações de apoio, plataformas educacionais contratadas, sistemas em nuvem ou fornecedores que realizem tratamento de dados pessoais em nome da instituição.

XI – produção ou classificação inadequada de documentos contendo dados pessoais
elaboração, registro, tramitação ou armazenamento de documentos físicos ou eletrônicos contendo dados pessoais sem a adoção de medidas adequadas de classificação da informação, definição de nível de acesso, restrição de compartilhamento, anonimização, pseudonimização ou observância do princípio da minimização, expondo informações pessoais além do necessário à finalidade administrativa.

Importa destacar que nem todo incidente de segurança da informação configura incidente sujeito à comunicação à ANPD. Eventos que não envolvam dados pessoais identificados ou identificáveis, ou que se restrinjam exclusivamente a dados anonimizados, não se enquadram, em regra, no dever de comunicação previsto na legislação.

Da mesma forma, a simples identificação de fragilidade técnica, falha de configuração ou vulnerabilidade em sistemas não caracteriza, por si só, incidente de segurança. Todavia, caso essa vulnerabilidade venha a ser explorada e resulte em comprometimento efetivo da segurança dos dados pessoais, estará configurado o incidente, devendo ser adotadas as providências previstas neste Guia.

Compete ao Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais, na qualidade de controlador de dados pessoais no âmbito de suas atividades institucionais, identificar, registrar, tratar, mitigar e avaliar os riscos decorrentes de incidentes de segurança, promovendo, quando cabível, a comunicação tempestiva à Autoridade Nacional de Proteção de Dados e aos titulares afetados, em observância aos princípios da prevenção, responsabilização, transparência e proteção integral dos dados pessoais.

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

A comunicação de incidente de segurança da informação com dados pessoais poderá ter origem interna ou externa, devendo sua formalização ocorrer de maneira célere, padronizada e documentada, a fim de viabilizar a pronta análise da ocorrência, a adoção das medidas de contenção necessárias, a preservação das evidências relacionadas ao evento e a implementação das providências institucionais cabíveis.

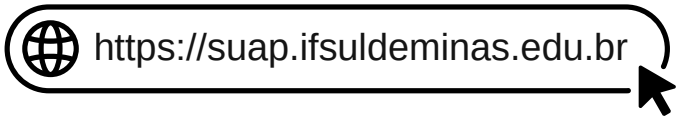
Durante o tratamento do incidente, deverão ser preservadas todas as evidências técnicas e administrativas relacionadas à ocorrência, incluindo logs de sistemas, registros de acesso, capturas de tela, documentos, comunicações institucionais, atas de reuniões, relatórios técnicos e demais elementos necessários à rastreabilidade das ações adotadas.

As evidências relacionadas ao incidente deverão ser preservadas de forma íntegra, rastreável e controlada, observando-se, sempre que aplicável, os princípios de cadeia de custódia digital, confidencialidade, integridade da informação e restrição de acesso aos registros produzidos durante a apuração e tratamento do incidente.

4.1 Notificação interna.

Quando identificado por servidor, colaborador, estudante, gestor, unidade administrativa ou equipe técnica do IFSULDEMINAS, o incidente deverá ser comunicado imediatamente por meio de Chamado no SUAP, adicionando as informações estipuladas para a abertura do chamado.

1 - ACESSAR SUAP



2 - ABRIR CHAMADO

3 - ESCOLHER A ÁREA DE TECNOLOGIA DA INFORMAÇÃO

4 - PREENCHER OS DADOS

A notificação deverá conter, sempre que possível:

I - Problema ocorrido:
II - Abrangência do incidente: exclusiva (somente com você) ou comum (afetou mais usuários).
III - Houve vazamento de dados? Se sim, houve vazamento de dados sensíveis?
IV - Há patrimônio institucional envolvido? Se sim, informar o(s) número(s) do(s) patrimônio(s).
V - Mais informações relevantes.

Anexar ao chamado documentos ou evidências que permitam subsidiar a análise do incidente, tais como relatórios, mensagens de correio eletrônico, capturas de tela (prints), registros de sistema, arquivos de log ou quaisquer outros elementos que contribuam para a identificação, compreensão e tratamento da ocorrência.

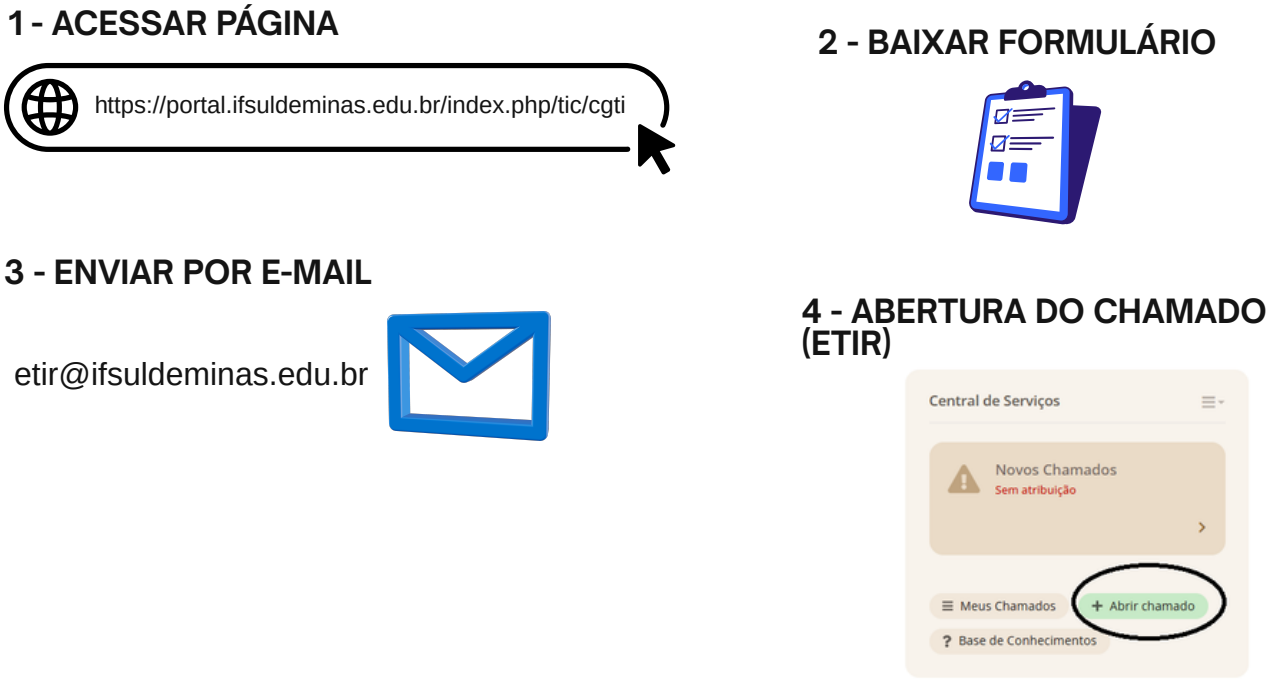
Após o registro do chamado, a comunicação será encaminhada imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, com ciência à Diretoria de Tecnologia da Informação, quando aplicável, à unidade gestora responsável pela base de dados afetada, para análise preliminar e adoção das medidas de contenção. O diagrama a seguir, apresenta o FLUXO DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS.

Havendo dados pessoais, deverá o Encarregado de Dados ser informado para tomar as devidas providências.

4.2 Notificação externa

Quando a comunicação do incidente tiver origem externa, o registro deverá ser feito por mei do e-mail: etir@ifsuldeminas.edu.br

Recebida a comunicação, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR avaliará a suficiência das informações apresentadas e, quando necessário, solicitará complementação ao comunicante. Ato contínuo, a ETIR procederá pela abertura formal do chamado.



4.3 Formalização e registro institucional

Após o recebimento do chamado, caso seja confirmado o envolvimento de dados pessoais, toda comunicação de incidente deverá ser formalizada em processo eletrônico institucional no SUAP, aberto pela ETIR-IFSULDEMINAS, com definição de nível de acesso restrito, observando-se os princípios da necessidade, da confidencialidade e da proteção dos dados envolvidos.

Conforme a natureza do incidente, poderão ser acionadas, de forma coordenada:
I – o Encarregado de dados;
II - a Ouvidoria, quando houver manifestação externa;
III – a Coordenação de Integridade e Controle Interno, quando houver repercussão institucional relevante;
IV – a Procuradoria Federal junto ao IFSULDEMINAS, quando necessária análise jurídica;
V – outras unidades administrativas competentes, conforme a especificidade do caso.
VI – o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, nos casos de incidentes cibernéticos que envolvam redes computacionais, infraestrutura tecnológica ou serviços digitais institucionais, observadas as diretrizes aplicáveis à Administração Pública Federal.

Nos casos de elevada criticidade, potencial impacto coletivo ou risco relevante aos titulares, o comitê de crise do IFSULDEMINAS deverá ser acionado para a adoção prioritária das medidas de contenção, mitigação e avaliação previstas neste Guia.

5. FLUXO SIMPLIFICADO DO RECEBIMENTO DA NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

IDENTIFICAÇÃO OU COMUNICAÇÃO

DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS (servidor, estudante, terceirizado, sistema, Ouvidoria, gestor, etc.

REGISTRO DA OCORRÊNCIA

Abertura de Chamado para a comunidade interna no SUAP e ou, preenchimento do Formulário (preferencialmente) e envio no e-mail etir@ifsuldeminas.edu.br

ANÁLISE E TRATAMENTO

A ETIR, conforme a natureza do caso, realiza a análise e o tratamento inicial do incidente e, havendo indícios de envolvimento de dados pessoais, comunica o Encarregado pelo Tratamento de Dados Pessoais - DPO.

COMUNICAÇÃO OU CONCLUSÃO

O DPO realiza, quando aplicável, as comunicações necessárias e acompanha a conclusão do processo.

No âmbito do IFSULDEMINAS, os incidentes de segurança da informação poderão ou não envolver dados pessoais, devendo sua caracterização ocorrer a partir de análise técnica e administrativa da ocorrência reportada.

Toda ocorrência relacionada à indisponibilidade, perda, alteração, divulgação não autorizada, acesso indevido, comprometimento de sistemas, falhas de segurança cibernética ou qualquer situação que represente risco aos ativos informacionais institucionais deverá ser formalizada conforme orientações presentes no item 4 deste Guia.

Compete ao ETIR-IFSULDEMINAS realizar a análise técnica preliminar da ocorrência, promovendo, quando necessário, as medidas de identificação, contenção, mitigação de riscos, preservação de evidências e avaliação da extensão do incidente, especialmente nos casos que envolverem sistemas computacionais, infraestrutura tecnológica, serviços digitais, redes institucionais ou demais ativos de tecnologia da informação.

Durante a análise preliminar, o ETIR-IFSULDEMINAS deverá avaliar a existência de indícios de comprometimento de dados pessoais, considerando os possíveis impactos à confidencialidade, integridade e disponibilidade das informações institucionais.

Quando houver indícios de envolvimento de dados pessoais digitais, o Encarregado pelo Tratamento de Dados Pessoais deverá ser acionado para atuação conjunta com o ETIR-IFSULDEMINAS e com a área responsável pela informação ou base de dados afetada, visando à avaliação da caracterização do incidente de segurança da informação com dados pessoais, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Caberá ao Encarregado apoiar a análise quanto à natureza e categoria dos dados pessoais afetados, ao quantitativo estimado de titulares envolvidos, aos potenciais riscos e impactos decorrentes, bem como à avaliação acerca da necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados, quando aplicável.

As áreas técnicas e administrativas envolvidas deverão complementar a análise sob os aspectos necessários à confirmação da ocorrência, extensão do incidente, medidas de contenção adotadas, riscos associados e demais elementos relevantes para subsidiar a tomada de decisão institucional.

Nos casos em que houver caracterização de incidente de segurança da informação com dados pessoais sujeito à comunicação, o Encarregado providenciará a ciência da Alta Administração do IFSULDEMINAS e adotará as providências necessárias para eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), com a Resolução CD/ANPD nº 15/2024 e demais normativos aplicáveis.

O resultado da análise será reportado em até três dias úteis via SUAP ao Encarregado na forma de Despacho. Em caso de caracterização de incidente de segurança com dados pessoais a ser comunicado, o Encarregado informará imediatamente ao Controlador do IFSULDEMINAS, após a ciência do Reitor, providenciará as comunicações pertinentes, conforme diagrama a seguir:

6. COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS À ANPD

O Encarregado pelo Tratamento de Dados Pessoais deverá comunicar o incidente de segurança à Autoridade Nacional de Proteção de Dados (ANPD) no prazo de até três dias úteis, contados do conhecimento, pelo controlador, de que o incidente afetou dados pessoais, observando os procedimentos disponibilizados no Peticionamento Eletrônico e na página oficial de comunicação de incidentes da ANPD.

A comunicação deverá ser acompanhada de comprovação do vínculo funcional do Encarregado, podendo ser utilizada a Declaração de Dados Funcionais (SouGov) juntamente com a Portaria de designação para a função.

O relatório encaminhado deverá conter, no mínimo, informações sobre a natureza dos dados afetados, quantitativo de titulares impactados, medidas de segurança adotadas, riscos e possíveis impactos aos titulares, medidas de mitigação, bem como a data da ocorrência e da ciência do incidente.

As informações poderão ser complementadas no prazo de até 20 dias úteis, mediante justificativa fundamentada. Nos casos que envolverem informações protegidas por sigilo legal, o controlador poderá solicitar à ANPD restrição de acesso às informações sensíveis apresentadas.

A ANPD poderá, a qualquer tempo, requisitar informações adicionais relacionadas ao incidente, incluindo registros de tratamento, RIPD e relatório de tratamento do incidente.

7. COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS AO TITULAR

A comunicação do incidente de segurança aos titulares de dados pessoais deverá ser realizada pelo IFSULDEMINAS, na condição de controlador, sendo a sua operacionalização conduzida pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio das áreas técnicas e administrativas competentes.

A mensagem deve utilizar linguagem simples, clara e acessível, preferencialmente de forma direta e individualizada (e-mail, telefone, carta etc.).

Quando não for possível identificar ou contatar os titulares individualmente, a divulgação deverá ocorrer por meios públicos, como site institucional, redes sociais e canais de atendimento, permanecendo visível por pelo menos três meses. Nesse caso, a Diretoria de Comunicação deverá ser acionada para operacionalizar a divulgação.

Também deverá ser juntada ao processo administrativo uma declaração comprovando a realização da comunicação aos titulares, indicando os meios utilizados.

Por fim, recomenda-se incluir orientações aos titulares sobre medidas para reduzir possíveis impactos do incidente, como boa prática prevista na LGPD.

8. REGISTRO DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

O IFSULDEMINAS, na condição de controlador, deverá manter registro formal de todos os incidentes de segurança da informação, inclusive daqueles não comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados pessoais, observadas as normas institucionais de gestão documental e as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade vigente.

O registro do incidente deverá ser formalizado e detalhado em processo administrativo no SUAP, sendo iniciado pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos do IFSULDEMINAS (ETIR-IFSULDEMINAS).

Os registros produzidos no âmbito do tratamento dos incidentes de segurança da informação constituem instrumentos de apoio à gestão da continuidade e do conhecimento institucional, permitindo a preservação do histórico das ocorrências, o compartilhamento de experiências, a identificação de padrões e o aprimoramento contínuo dos procedimentos, controles e práticas relacionadas à privacidade e à segurança da informação no âmbito do IFSULDEMINAS.

Após a conclusão das medidas de tratamento, contenção e mitigação do incidente, envolvendo dados pessoais, deverá ser elaborado relatório final contendo a consolidação das informações técnicas e administrativas relacionadas à ocorrência, incluindo medidas adotadas, impactos identificados, comunicações realizadas, evidências produzidas e recomendações preventivas.

O relatório final deverá subsidiar ações de melhoria contínua relacionadas à governança de privacidade e segurança da informação, podendo ensejar revisão de procedimentos, controles internos, avaliações de risco, Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e demais instrumentos institucionais aplicáveis.

9. DISPOSIÇÕES FINAIS

As orientações contidas neste documento são de observância obrigatória pelas unidades do IFSULDEMINAS envolvidas no processo de tratamento, resposta e comunicação de incidentes de segurança da informação, especialmente aqueles que envolvam dados pessoais.

Este documento deverá possuir ampla divulgação institucional, tanto por meio do portal eletrônico do IFSULDEMINAS quanto pelos canais oficiais de comunicação interna e externa, incluindo correio eletrônico institucional e demais meios administrativos utilizados pela instituição.

Havendo necessidade de revisão deste documento, a proposta poderá ser encaminhada pela unidade proponente para análise institucional, com manifestação do ETIR-IFSULDEMINAS, do Encarregado pelo Tratamento de Dados Pessoais e das demais áreas competentes relacionadas à governança de privacidade, segurança da informação e gestão de riscos institucionais.

10. ANEXO I - DEFINIÇÕES

Para os fins deste **GUIA DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS NO ÂMBITO DO IFSULDEMINAS**, adotam-se as seguintes definições:

AMPLA DIVULGAÇÃO DO INCIDENTE medida excepcional de comunicação pública que poderá ser adotada ou determinada pela Autoridade Nacional de Proteção de Dados, quando cabível, com o objetivo de dar transparência à ocorrência, podendo ocorrer por meio do portal institucional, canais oficiais de comunicação, redes sociais institucionais ou outros meios adequados ao alcance dos titulares impactados.

AUTENTICIDADE atributo que assegura a legitimidade da origem de uma informação, garantindo que sua criação, alteração, transmissão ou exclusão decorreu de agente, sistema ou processo devidamente identificado e autorizado.

CATEGORIA DE DADOS PESSOAIS agrupamento dos dados pessoais segundo sua natureza, finalidade de uso ou contexto de tratamento, podendo compreender, entre outros, dados cadastrais, financeiros, acadêmicos, funcionais, biométricos e credenciais de acesso a sistemas.

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA procedimento formal pelo qual o controlador informa a ocorrência de incidente de segurança à Autoridade Nacional de Proteção de Dados e, quando aplicável, aos titulares dos dados, especialmente quando houver possibilidade de risco ou dano relevante.

CONFIDENCIALIDADE princípio de proteção da informação que assegura que dados pessoais somente sejam acessados, utilizados ou conhecidos por pessoas, sistemas ou unidades devidamente autorizados.

DADO DE AUTENTICAÇÃO EM SISTEMAS informação pessoal utilizada para validação de identidade ou concessão de acesso a ambientes tecnológicos, incluindo, exemplificativamente, login institucional, senha, token, certificado digital ou outro mecanismo de autenticação.

DADO FINANCEIRO informação pessoal relacionada à vida econômica do titular, abrangendo registros bancários, remuneração, benefícios, bolsas, pagamentos, reembolsos ou outras movimentações de natureza financeira.

DADO PESSOAL AFETADO dado pessoal alcançado por incidente de segurança que resulte, potencial ou efetivamente, em comprometimento de sua confidencialidade, integridade, disponibilidade ou autenticidade.

DADO PESSOAL SENSÍVEL categoria especial de dado pessoal que, em razão de sua natureza, demanda maior proteção, incluindo informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, genética ou biometria vinculada à pessoa natural.

DADO SOB SIGILO LEGAL, JUDICIAL OU PROFISSIONAL informação pessoal submetida a regime específico de restrição de acesso ou divulgação em razão de previsão normativa, decisão judicial ou dever de sigilo decorrente de função, ofício ou profissão.

DADOS EM LARGA ESCALA conjunto expressivo de dados pessoais que envolva número significativo de titulares ou tratamento com elevada abrangência quanto a volume, frequência, duração ou alcance territorial.

DISPONIBILIDADE garantia de que os dados pessoais permaneçam acessíveis e utilizáveis, no momento necessário, por agentes, unidades ou sistemas autorizados.

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS ocorrência confirmada que provoque, ou tenha potencial de provocar, comprometimento da proteção de dados pessoais, por meio de acesso indevido, perda, alteração, indisponibilidade, vazamento, destruição ou qualquer evento que afete sua segurança.

INTEGRIDADE característica que assegura a exatidão, completude e preservação do conteúdo dos dados pessoais, impedindo alterações, supressões ou corrupções não autorizadas.

MEDIDAS DE SEGURANÇA conjunto de controles administrativos, técnicos, físicos e organizacionais implementados para prevenir, detectar, responder e mitigar riscos relacionados ao tratamento inadequado ou ilícito de dados pessoais.

NATUREZA DOS DADOS PESSOAIS classificação dos dados pessoais conforme o grau de sensibilidade atribuído pela legislação, distinguindo-se, de forma geral, entre dados pessoais comuns e dados pessoais sensíveis.

RELATÓRIO DE TRATAMENTO DE INCIDENTE registro técnico e administrativo elaborado após a identificação de incidente, contendo descrição da ocorrência, análise de impacto, evidências coletadas, providências adotadas, medidas corretivas implementadas e avaliação quanto à necessidade de comunicação aos órgãos competentes e aos titulares envolvidos.

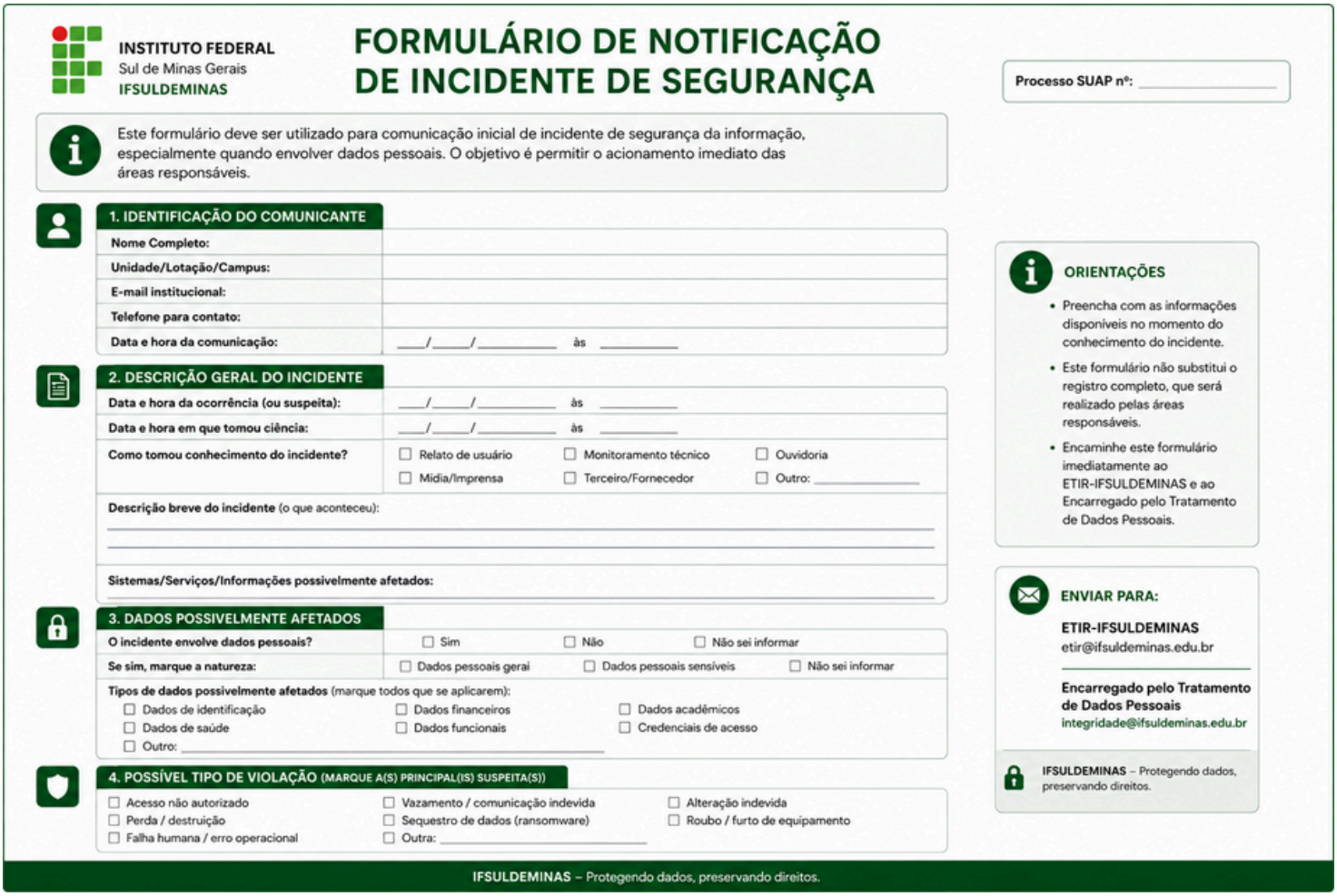
11- ANEXO II - PAPÉIS E RESPONSABILIDADES

ÁREA	RESPONSABILIDADES
Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR	• Coordenar as atividades de tratamento e resposta a incidentes de SI, adotando todas as medidas reativas e corretivas necessárias, nos termos da Política de Segurança da Informação do IFSULDEMINAS • Analisar o incidente de segurança da informação com dados pessoais e gerar relatório de tratamento de incidente, encaminhando-o ao Encarregado em até três dias úteis; • Instruir o respectivo processo com o registro do incidente de segurança de que trata o art. 10 da Resolução CD/ANPD N.º 15/2024.
Diretoria de Tecnologia da Informação - DTI	• Prestar suporte técnico e operacional à ETIR-IFSULDEMINAS na execução das medidas de tratamento e resposta ao incidente, incluindo análise de infraestrutura, disponibilização de registros, implementação de medidas corretivas, recuperação de serviços e demais ações necessárias à efetivação das deliberações e encaminhamentos definidos pela ETIR-IFSULDEMINAS
Encarregado pelo Tratamento de Dados Pessoais - DPO	• Receber, na condição de canal de comunicação do controlador, notificações de incidentes de segurança envolvendo dados pessoais encaminhadas interna ou externamente; • Articular e acompanhar o fluxo de tratamento do incidente junto à ETIR-IFSULDEMINAS, DTI e demais unidades envolvidas, quando aplicável; • Apoiar a análise da necessidade de comunicação à ANPD e aos titulares dos dados pessoais, bem como, quando aplicável, coordenar a divulgação institucional do incidente por meio dos canais oficiais do IFSULDEMINAS, observados os requisitos legais e normativos aplicáveis. • Articular e acompanhar junto à ETIR-IFSULDEMINAS, DTI e demais unidades envolvidas, quando aplicável a elaboração do relatório final do tratamento realizado;

11 - ANEXO II - PAPÉIS E RESPONSABILIDADES

ÁREA	RESPONSABILIDADES
Diretoria de Comunicação - DICOM	• Realizar comunicação ampla em caso de incidente em que não seja viável a comunicação direta e individualizada, conforme §3.º, art. 9.º da Resolução CD/ANPD N.º 15/2024.
Coordenação de Integridade e Controle Interno - COI	• Apoiar a governança institucional do processo de comunicação, tratamento e acompanhamento de incidentes de segurança da informação com dados pessoais, quando houver repercussão institucional relevante. • Contribuir para a revisão e atualização deste Guia, sempre que identificadas necessidades de aprimoramento relacionadas aos processos de governança, integridade, privacidade e segurança da informação.

12 - ANEXO III- FORMULÁRIO DE NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA



INSTITUTO FEDERAL
Sul de Minas Gerais
IFSULDEMINAS

FORMULÁRIO DE NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA

Processo SUAP nº: _____

Este formulário deve ser utilizado para comunicação inicial de incidente de segurança da informação, especialmente quando envolver dados pessoais. O objetivo é permitir o acionamento imediato das áreas responsáveis.

1. IDENTIFICAÇÃO DO COMUNICANTE

Nome Completo:	
Unidade/Lotação/Campus:	
E-mail institucional:	
Telefone para contato:	
Data e hora da comunicação:	___/___/_____ às _____

2. DESCRIÇÃO GERAL DO INCIDENTE

Data e hora da ocorrência (ou suspeita):	___/___/_____ às _____
Data e hora em que tomou ciência:	___/___/_____ às _____
Como tomou conhecimento do incidente?	☐ Relato de usuário ☐ Monitoramento técnico ☐ Ouvidoria ☐ Mídia/Imprensa ☐ Terceiro/Fornecedor ☐ Outro: _____

Descrição breve do incidente (o que aconteceu):

_____

_____

Sistemas/Serviços/Informações possivelmente afetados:

_____

3. DADOS POSSIVELMENTE AFETADOS

O incidente envolve dados pessoais?	☐ Sim ☐ Não ☐ Não sei informar
Se sim, marque a natureza:	☐ Dados pessoais gerai ☐ Dados pessoais sensíveis ☐ Não sei informar

Tipos de dados possivelmente afetados (marque todos que se aplicarem):

☐ Dados de identificação ☐ Dados financeiros ☐ Dados acadêmicos
☐ Dados de saúde ☐ Dados funcionais ☐ Credenciais de acesso
☐ Outro: _____

4. POSSÍVEL TIPO DE VIOLAÇÃO (MARQUE A(S) PRINCIPAL(IS) SUSPEITA(S))

☐ Acesso não autorizado ☐ Vazamento / comunicação indevida ☐ Alteração indevida
☐ Perda / destruição ☐ Sequestro de dados (ransomware) ☐ Roubo / furto de equipamento
☐ Falha humana / erro operacional ☐ Outra: _____

ORIENTAÇÕES

- Preencha com as informações disponíveis no momento do conhecimento do incidente.
- Este formulário não substitui o registro completo, que será realizado pelas áreas responsáveis.
- Encaminhe este formulário imediatamente ao ETIR-IFSULDEMINAS e ao Encarregado pelo Tratamento de Dados Pessoais.

ENVIAR PARA:

ETIR-IFSULDEMINAS
etir@ifsuldeminas.edu.br

Encarregado pelo Tratamento de Dados Pessoais
integridade@ifsuldeminas.edu.br

IFSULDEMINAS – Protegendo dados, preservando direitos.

IFSULDEMINAS – Protegendo dados, preservando direitos.

Documento Digitalizado Público

Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais no âmbito do IFSULDEMINAS.

Assunto: Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais no âmbito do IFSULDEMINAS.
Assinado por: Pamela Oliveira
Tipo do Documento: Documento
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Pamela Helia de Oliveira**, **COORDENADOR(A) GERAL - CD4 - IFSULDEMINAS - COI**, em 15/06/2026 09:20:53.

Este documento foi armazenado no SUAP em 16/06/2026. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 847515
Código de Autenticação: 7006e0981b