Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS DO IFMS

INSTITUTO FEDERAL
Mato Grosso do Sul

Missão

Promover a educação de excelência por meio do ensino, pesquisa e extensão nas diversas áreas do conhecimento técnico e tecnológico, formando profissional humanista e inovador, com vistas a induzir o desenvolvimento econômico e social local, regional e nacional.

Visão

Ser reconhecido como uma instituição de ensino de excelência, sendo referência em educação, ciência e tecnologia no Estado de Mato Grosso do Sul.

Valores

Inovação;
Ética;
Compromisso com o desenvolvimento local e regional;
Transparência;
Compromisso Social.

INSTITUTO FEDERAL
Mato Grosso do Sul

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO DO SUL IFMS	
Endereço:	Rua Jornalista Belizário Lima, 236 - Campo Grande - MS CEP: 79.004-270
CNPJ:	10.673.078/0001-20

identificação	
PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS DO IFMS	
Elaborado por:	Diretoria de Gestão Sistêmica, Governança, Riscos, Transparência e Inovação Pública; Diretoria de tecnologia da Informação; Ouvidoria.
Data de publicação:	Dezembro/2025

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS DO INSTITUTO FEDERAL DE MATO GROSSO DO SUL

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) estabelece que os agentes de tratamento de dados têm o dever de assegurar a segurança das informações sob sua responsabilidade, conforme o disposto no artigo 47. Essa obrigação de proteção permanece vigente mesmo após o encerramento do tratamento dos dados. A inexistência de medidas técnicas e administrativas adequadas para garantir essa segurança pode ocasionar danos equivalentes aos resultantes de ataques cibernéticos.

O artigo 46 da LGPD reforça a necessidade de adoção de precauções destinadas a resguardar os dados pessoais contra acessos não autorizados, incidentes acidentais ou formas inadequadas de tratamento. Tais precauções vão além da utilização de tecnologias e padrões de segurança, abrangendo também a elaboração, manutenção e revisão de documentos institucionais. Essas práticas contribuem para o aperfeiçoamento dos processos internos e para a proteção da reputação da instituição, bem como de seus servidores, colaboradores e prestadores de serviço.

Este guia foi elaborado com fundamento na Resolução nº 15/2024 da Autoridade Nacional de Proteção de Dados (ANPD), com o propósito de orientar os setores responsáveis pelo tratamento de dados pessoais e demais servidores do Instituto Federal de Mato Grosso do Sul (IFMS). O documento enfatiza a importância da resposta célere a incidentes de segurança e a preservação dos direitos dos titulares.

Busca-se, com isso, incentivar a adoção de boas práticas de segurança e proteção de dados, especialmente no que se refere à resposta a incidentes. As informações contidas neste guia serão periodicamente revisadas e atualizadas, de modo a incorporar melhorias contínuas, novas normas e diretrizes, acompanhando a evolução das políticas e processos institucionais de proteção de dados pessoais.

2. Objetivos

- **Geral:** Estabelecer diretrizes e fluxos para identificação, resposta e comunicação de incidentes, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.
- **Específicos:**
- Garantir a conformidade com a Lei nº 13.709/2018 – LGPD;
- Proteger a imagem institucional;
- Assegurar a rastreabilidade e transparência; e
- Fomentar a cultura organizacional de segurança e proteção de dados.

3. Definições

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões e responsabilidades referentes ao tratamento de dados pessoais. Para clareza desta definição, o papel de controlador é atribuído à União e ao Instituto Federal de Mato Grosso do Sul, por força do princípio da desconcentração administrativa, e, portanto, devem observar as obrigações impostas pela LGPD.

Controlador-Conjunto: definem, em conjunto, os processos e as finalidades do tratamento por interesse mútuo, e respondem solidariamente por suas decisões e responsabilidades.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Recurso criptográfico - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

Agentes de tratamento: o controlador e o operador

Encarregado: pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD). No âmbito do IFMS, esta função está atribuída ao (a) ouvidor (a);

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

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

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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;

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.

4. Estrutura Organizacional e Responsabilidades

Dentre os principais responsáveis, em caso de incidente de segurança envolvendo o tratamento de dados pessoais, identificam-se a seguir aqueles que atuarão diretamente no processo de trabalho descrito neste Plano.

O Comitê de Governança Digital (CGD): de natureza consultiva e deliberativa, tem por finalidade o alinhamento das ações de Tecnologia da Informação e Comunicação – TIC

ao acompanhamento dos dados abertos e da transformação digital, considerando para tanto o disposto no Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC.

O Comitê de Segurança de Tecnologia da Informação e Comunicação (CSTIC): Órgão colegiado de natureza consultiva, propositiva e de caráter permanente, com a finalidade de planejar e coordenar as atividades de segurança da informação e comunicação no âmbito do IFMS

Encarregado pelo Tratamento de Dados Pessoais: Atua como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD). No âmbito do IFMS, esta função está atribuída ao (a) ouvidor (a);

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, deve notificar imediatamente o encarregado em caso de suspeita ou confirmação de incidente.

Diretoria de Tecnologia da Informação: Atua na contenção e recuperação técnica.

5. Incidente de Segurança com Dados Pessoais

Conforme a Resolução nº 15/2024 da ANPD, incidente de segurança é qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

Esses incidentes podem ser causados por ações maliciosas, ataques cibernéticos ou furto de dispositivos de armazenamento. Também podem ser causados por eventos não

intencionais, como erros humanos ou falhas de sistema. Tais ocorrências podem representar riscos significativos para os direitos e liberdades dos titulares dos dados.

6. Critérios para Comunicação de Incidente de Segurança

O controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - Dados pessoais sensíveis;

II - Dados de crianças, de adolescentes ou de idosos;

III - Dados financeiros;

IV - Dados de autenticação em sistemas;

V - Dados protegidos por sigilo legal, judicial ou profissional; ou

VI - dados em larga escala.

O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

7. Procedimentos em Caso de Incidente

1) Notificação do Incidente:

Um novo incidente de segurança pode ser notificado por pessoa externa ou interna, podendo ser operador, titular ou cidadão ao encarregado. Recomenda-se

que a notificação seja feita por um desses meios: ouvidoria@ifms.edu.br ou Plataforma Integrada de Ouvidoria e Acesso à Informação - https://falabr.cgu.gov.br/.

Se recebido por outros meios, a notificação deverá ser encaminhada ao e-mail ouvidoria@ifms.edu.br

2) Abertura de Processo

Após recebimento da ocorrência pelo encarregado, este deverá proceder abertura do processo no Sistema Unificado de Administração Pública (Suap).

3) Avaliação Preliminar

A notificação será encaminhada à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) vinculada à DIRTI, que deverá:

- Avaliar se há elementos que comprovem o incidente de segurança de dados pessoais;
- Avaliar previamente o incidente para obter informações iniciais sobre o impacto do ocorrido, identificando a origem; categoria; quantidade de titulares e de dados pessoais afetados.

4) Avaliação técnica

Havendo elementos técnicos que comprovem o incidente pela ETIR, a Diretoria de Tecnologia da Informação - DIRTI é responsável pela documentação com a avaliação interna do incidente, indicando:

- Qual vulnerabilidade foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.
- A avaliação do impacto que o incidente pode gerar aos titulares;

- As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os dados sigilosos.
- Levantamento e análise dos riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
- Encaminhamento da avaliação técnica para o encarregado da LGPD.

5) Ciência do Controlador e Autorização de Comunicação

Após a avaliação técnica pela a Diretoria de Tecnologia da Informação que confirma o incidente, o encarregado comunicará oficialmente o controlador (Autoridade Máxima), que dará ciência da ocorrência e autorização de comunicação de incidente de Segurança de Dados Pessoais ao encarregado.

6) Comunicação à ANPD e aos Titulares

Após ciência do controlador, o encarregado terá um prazo de 3 dias para comunicar à ANPD:

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 previsto no caput deste artigo;
VI. As 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 a determinar, 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; e
XII. Do total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Após ciência do controlador, o encarregado terá um prazo de 3 dias para comunicar aos titulares:

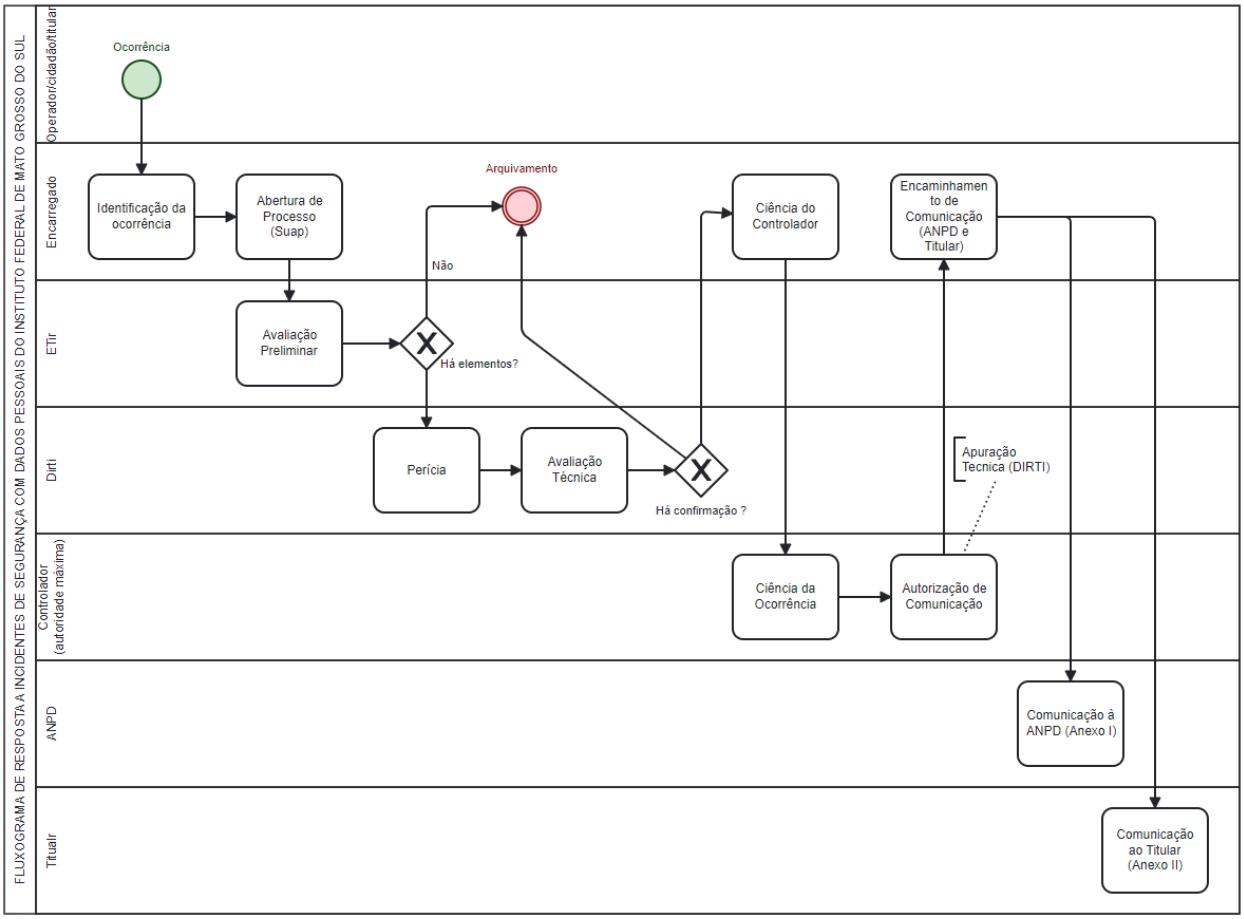
I. A descrição da natureza e da categoria de dados pessoais afetados;
II. As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
III. Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
IV. Os motivos 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.

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

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

8. Fluxograma do Processo

Inclui o fluxograma visual mostrando o caminho do incidente desde a identificação até a extinção do processo, destacando a Ouvidoria como Encarregada de Dados



9. Relatório Final do Incidente

Esta etapa final tem como objetivo registrar de forma detalhada a ocorrência do incidente e as providências adotadas, mediante a elaboração de um relatório circunstanciado, que consolide todas as informações relevantes sobre o evento. O documento deverá conter, obrigatoriamente, a descrição da causa raiz, o impacto identificado, as medidas corretivas e preventivas adotadas, bem como os prazos previstos para implementação e acompanhamento das ações.

Tal relatório permitirá ao IFMS adotar medidas preventivas e corretivas eficazes, voltadas à mitigação de riscos e à prevenção de novos episódios que envolvam vulnerabilidades tecnológicas ou falhas operacionais.

O relatório final tem por objetivos:

- Avaliar o processo de tratamento do incidente e verificar a eficácia das soluções implementadas;

- Identificar a causa raiz do incidente e avaliar seus impactos técnicos, operacionais, reputacionais e de conformidade;

- Relacionar e documentar eventuais falhas, lacunas ou recursos inexistentes ou insuficientes, de modo que possam ser providenciados em futuras situações;

- Descrever as medidas adotadas para contenção, erradicação e recuperação, bem como as ações preventivas planejadas, indicando responsáveis e prazos para sua execução;

- Compartilhar as lições aprendidas com outros setores institucionais, quando pertinente, a fim de promover o aperfeiçoamento contínuo da infraestrutura tecnológica e dos processos de resposta a incidentes;

- Comunicar às áreas afetadas as decisões e recomendações decorrentes do processo, visando aprimorar as práticas de segurança e reduzir a probabilidade de recorrência de incidentes da mesma natureza; e

- Realizar os ajustes necessários na Governança em Privacidade do IFMS, assegurando sua conformidade com as normas, resoluções da ANPD e boas práticas de proteção de dados pessoais.

10. Anexos

- Anexo I – Formulário de Comunicação de Incidente de Segurança do IFMS
- Anexo II – Formulário de Comunicação ao Titular.
- Anexo III – Modelo de Relatório Final

Anexo I

Razão Social	Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul		
CNPJ	10.673.078/0001-20		
Endereço	Rua Jornalista Belizário Lima nº 236		
Cidade:	Campo Grande	Estado:	Mato Grosso do Sul
CEP:	79.004-270		
Telefone:	(67) 3378-9500	E-mail:	reitoria@ifms.edu.br

Dados do Encarregado

Possui um encarregado pela proteção de dados pessoais?	☐ Sim	☐ Não
Nome:		
CNPJ/CPF:		
Telefone:	E-mail:	

Representante Legal da Instituição

Nome:
CNPJ/CPF:
Telefone:
E-mail:

Descrição do Incidente

Data da ocorrência:

Dados Pessoais Afetados:	
Quantidade Estimada de Titulares Afetados:	
Medidas Adotadas pelo IFMS:	

Avaliação dos riscos

Possíveis riscos aos Titulares:	
Orientações para mitigação dos riscos:	

Anexo II

Formulário de Comunicação de Incidente de Segurança com Dados Pessoais ao titular

Dados do Controlador

Razão Social	Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul		
CNPJ	10.673.078/0001-20		
Endereço	Rua Jornalista Belizário Lima nº 236		
Cidade:	Campo Grande	Estado:	Mato Grosso do Sul
CEP:	79.004-270		
Telefone:	(67) 3378-9500	E-mail:	reitoria@ifms.edu.br

Dados do Encarregado

Possui um encarregado pela proteção de dados pessoais?	☐ Sim	☐ Não
Nome:		
CNPJ/CPF:		
Telefone:	E-mail:	

Representante Legal da Instituição

Nome:
CNPJ/CPF:
Telefone:
E-mail:

Descrição do Incidente

Data da ocorrência:	
Dados Pessoais Afetados:	
Quantidade Estimada de Titulares Afetados:	
Medidas Adotadas pelo IFMS:	

Avaliação dos riscos

Possíveis riscos aos Titulares:	
Orientações para mitigação dos riscos:	

Canal de Contato para Suporte

E-mail:	
Telefone:	

Anexo III

Modelo de Relatório Final de Comunicação de Incidente de Segurança com Dados Pessoais

Dados do Controlador		
Razão Social	Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul	
CNPJ	10.673.078/0001-20	
Endereço	Rua Jornalista Belizário Lima nº 236	
Cidade:	Campo Grande	Estado: Mato Grosso do Sul
CEP:	79.004-270	
Telefone:	(67) 3378-9500	E-mail: reitoria@ifms.edu.br
Informe o número aproximado de titulares cujos dados são tratados por sua organização:		
Dados do Encarregado		
Possui um encarregado pela proteção de dados pessoais?	☐ Sim	☐ Não
Nome:		
CNPJ/CPF:		
Telefone:	E-mail:	
Representante Legal da Instituição		
Nome:		
CNPJ/CPF:		
Telefone:		
E-mail:		
Tipo de Comunicação		
☐ Completa	*Todas as informações a respeito do incidente estão disponíveis e* ***a comunicação aos titulares já foi realizada****.*	
☐ Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a* ***comunicação aos titulares ainda não foi realizada****.* *A complementação deverá ser encaminhada no prazo de* ***20 dias úteis*** *a contar da data da comunicação* – Art. 6º § 3º do Regulamento de Comunicação de Incidentes.	
☐ Complementar	*Complementação de informações prestadas em comunicação preliminar.*	
Avaliação do Risco do Incidente		
☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.		
☐ O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**		
☐ O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)**		

Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente

☐ Identificado pelo próprio controlador.	☐ Notícias ou redes sociais.
☐ Notificação do operador de dados.	☐ Notificação da ANPD.
☐ Denúncia de titulares/terceiros	☐ Outros. (especifique)

Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:

Caso o incidente tenha sido comunicado ao controlador por um operador, informe:

Dados do Operador

Razão Social / Nome:

CNPJ/CPF:

E-mail:

Da Tempestividade da Comunicação do Incidente

Informe as seguintes datas, sobre o incidente:

Quando ocorreu

Quando tomou ciência

Quando comunicou à ANPD

Quando comunicou aos titulares

Justifique, se cabível, a não realização da comunicação à ANPD e aos titulares de dados afetados no prazo de 3 (três) dias úteis conforme prevê o Art. 6º da Resolução CD/ANPD nº 15, de 24 de abr de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança.

Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:

Da Comunicação do Incidente aos Titulares dos Dados

Os titulares dos dados afetados foram comunicados sobre o incidente?

☐ Sim.	☐ Não, por não haver risco ou dano relevante a eles.
☐ Não, mas o processo de comunicação está em andamento.	☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)

Se cabível, quando os titulares serão comunicados sobre o incidente?

De que forma a ocorrência do incidente foi comunicada aos titulares?

☐ Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*	☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
☐ Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*	☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*Especifique abaixo*)
☐ Outros. (*especifique abaixo*)	☐ Não se aplica.

Descreva como ocorreu a comunicação:

Quantos titulares foram comunicados individualmente sobre o incidente?

Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:

O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:

1. Resumo e data de ocorrência do incidente;
2. Descrição dos dados pessoais afetados;
3. Riscos e consequências aos titulares de dados;
4. Medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis; dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

O comunicado aos titulares atendeu os requisitos acima?

☐ Sim	☐ Não

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)

☐ Sequestro de Dados (*ransomware*) sem transferência de informações.	☐ Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
☐ Exploração de vulnerabilidade em sistemas de informação.	☐ Vírus de Computador / *Malware*.
☐ Roubo de credenciais / Engenharia Social.	☐ Violação de credencial por força bruta.

☐ Publicação não intencional de dados pessoais.	☐ Divulgação indevida de dados pessoais.
☐ Envio de dados a destinatário incorreto.	☐ Acesso não autorizado a sistemas de informação.
☐ Negação de Serviço (DoS).	☐ Alteração/exclusão não autorizada de dados.
☐ Perda/roubo de documentos ou dispositivos eletrônicos.	☐ Descarte incorreto de documentos ou dispositivos eletrônicos.
☐ Falha em equipamento (hardware).	☐ Falha em sistema de informação (*software*).
☐ Outro tipo de incidente cibernético. (especifique abaixo)	☐ Outro tipo de incidente não cibernético. (especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):

☐ Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
☐ Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
☐ Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)

☐ Origem racial ou étnica.	☐ Convicção religiosa.	☐ Opinião política.
☐ Referente à saúde.	☐ Biométrico.	☐Genético.
☐ Referente à vida sexual.	☐ Filiação a organização sindical, religiosa, filosófica ou política.	

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)

☐ Dados básicos de identificação *(ex.: nome, sobrenome, data de nascimento, matrícula)*	☐ Número de documentos de identificação oficial. *(ex.: RG, CPF, CNH, passaporte)*	☐ Dados de contato. (*ex.: telefone, endereço, e-mail*)
☐ Dados de meios de pagamento.	☐ Cópias de documentos de identificação oficial.	☐ Dados protegidos por sigilo profissional/legal.

(ex.: cartão de crédito/débito)		
☐ Dado financeiro ou econômico.	☐ Nomes de usuário de sistemas de informação.	☐ Dado de autenticação de sistema. (*ex.: senhas, PIN ou tokens)*
☐ Imagens / Áudio / Vídeo	☐ Dado de geolocalização. *(ex.: coordenadas geográficas)*	☐ Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados

Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?

☐ Sim	☐ Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?

Qual a quantidade aproximada de titulares afetados[1] pelo incidente?
Total de titulares afetados
Crianças e/ou adolescentes
Outros titulares vulneráveis

Se aplicável, descreva as categorias de titulares vulneráveis afetados:

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)		
☐ Funcionários.	☐Prestadores de serviços.	☐ Estudantes/Alunos.
☐ Clientes/Cidadãos.	☐ Usuários.	☐ Inscritos/Filiados.
☐ Pacientes de serviço de saúde.	☐Ainda não identificadas.	☐ Outros. (especifique abaixo)

[1] Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.

Informe o quantitativo de titulares afetados, por categoria:

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)

☐ Danos morais.	☐ Danos materiais.	☐ Violação à integridade física
☐ Discriminação social.	☐ Danos reputacionais.	☐ Roubo de identidade.
☐ Engenharia social / Fraudes.	☐ Limitação de acesso a um serviço.	☐ Exposição de dados protegidos por sigilo profissional/legal.
☐ Restrições de direitos.	☐ Perda de acesso a dados pessoais.	☐ Outros (especifique abaixo).

Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:

Qual o provável impacto do incidente sobre os titulares?

Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

☐ Sim, integralmente protegidos por criptografia / pseudonimização.	☐ Sim, parcialmente protegidos por criptografia / pseudonimização.	☐ Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas?

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐Atualização de Sistemas.

☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.
☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança?

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐Atualização de Sistemas.
☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:

As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?

☐ Sim ☐ Não

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>