



UFU

Universidade
Federal de
Uberlândia

GUIA

DE COMUNICAÇÃO DE

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

COM DADOS PESSOAIS NA UFU

<http://www.ufu.br/clgpd> | dpo@ufu.br

Fevereiro de 2026

GUIA DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS NA UFU

1. APRESENTAÇÃO

A **Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018**, determina, no Art. 48, *caput*, que "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." Tal disposição da LGPD foi regulamentada pela Agência Nacional de Proteção de Dados (ANPD), por meio da **Resolução CD/ANPD Nº 15, de 24/04/2024**, que aprova o **Regulamento de Comunicação de Incidente de Segurança** (<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>).

O **Regulamento de Comunicação de Incidente de Segurança** supramencionado "tem por objetivo estabelecer os procedimentos para Comunicação de Incidente de Segurança, que possa acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)".

Cabe registrar que esse tema integra a determinação do Tribunal de Contas da União (TCU), prevista no Acórdão nº 1372/2025/TCU /Plenário, para que 250 organizações, dentre as quais a UFU, "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*".

O presente **Guia de Comunicação de Incidente de Segurança da Informação com Dados Pessoais na Universidade Federal de Uberlândia** foi elaborado no âmbito da Comissão de Análise e Implementação da Lei Geral de Proteção de Dados Pessoais na Universidade Federal de Uberlândia - CLGPD/UFU - Portaria de Pessoal UFU Nº 8.248, de 22 de dezembro de 2025 (<https://ufu.br/unidades-organizacionais/comissao-de-analise-e-implementacao-da-lei-geral-de-protecao-de-dados>) e aprovado pelo Comitê de Governança Digital da Universidade Federal de Uberlândia – CGD/UFU (<https://ufu.br/unidades-organizacionais/comite-de-governanca-digital>), órgão criado pela Resolução nº 3/2020 do Conselho Diretor da Universidade Federal de Uberlândia – CONDIR/UFU, para deliberar sobre assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação (<http://www.reitoria.ufu.br/Resolucoes/resolucaoCONDIR-2020-3.pdf>).

2. DEFINIÇÕES

Para fins de aplicação deste Guia, serão adotadas as definições apresentadas a seguir, constantes na **Resolução CD/ANPD Nº 15, de 24 de abril de 2024**, e na **Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018**, no que se refere a incidentes ocorridos nos órgãos da administração pública federal.

- **agentes de tratamento:** o **controlador** (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e o **operador** (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador);
- **ampla divulgação do incidente em meios de comunicação:** providência que pode ser determinada pela Agência Nacional de Proteção de Dados (ANPD) ao controlador, nos termos do Art. 48, § 2º, Inciso I, da LGPD, no âmbito do processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do controlador ou em outros meios de comunicação;
- **autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- **categoria de dados pessoais:** classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;
- **comunicação de incidente de segurança:** ato 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;
- **confidencialidade:** propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados;
- **dado de autenticação em sistemas:** qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas;
- **dado financeiro:** dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;

- **dado pessoal afetado:** dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;
- **dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **dado protegido por sigilo legal ou judicial:** dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;
- **dado protegido por sigilo profissional:** dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;
- **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;
- **disponibilidade:** propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;
- **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD;
- **incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;
- **integridade:** propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental;
- **medidas de segurança:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **natureza dos dados pessoais:** classificação de dados pessoais em gerais ou sensíveis;
- **relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar

riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

- **relatório de tratamento de incidente:** documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos;
- **titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3. O QUE CARACTERIZA UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

De acordo com o **Regulamento de Comunicação de Incidente de Segurança da ANPD (Resolução CD/ANPD Nº 15, de 24/04/2024)**, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares deve ser comunicada à ANPD e ao titular dos dados pessoais, pelo controlador; e estabelece o seguinte:

Art. 5º 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.

§ 1º 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.

§ 2º 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.

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

A notificação sobre o incidente de segurança com dados pessoais na UFU deverá ser feita via Plataforma Integrada de Ouvidoria e Acesso à Informação – Fala.BR, cujas instruções para registro de manifestações estão disponíveis no site da Ouvidoria-Geral da UFU (https://ufu.br/sites/default/files/2025-09/tutorial-para-registro-de-manifestacao-na-plataforma-fala.br_.pdf).

A pessoa demandante deverá preencher e anexar o **"Formulário de Notificação de Incidente de Segurança ao Encarregado"** na Plataforma Fala.BR, junto à manifestação (**Anexo I** deste Guia, *versão* *editável* *disponível* *em*: https://sei.ufu.br/sei/controlador.php?acao=procedimento_trabalhar&id_procedimento=7846517 e em https://sei.ufu.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?il3OtHvPArITY997V09rhsSkbDKbaYSycOHqqF2xsM0laDkkEyJpus7kCPb435VNEAb16AAxmJKUdrsNWVlqQ4qHWXX7Blo0nFSr9Feiauykbqz8rTphpKi3KY26ZTAn).

Além do Formulário, poderão ser anexados outros documentos eletrônicos que comprovem e caracterizem o incidente de segurança. A Equipe da Ouvidoria-Geral da UFU remeterá a demanda ao Encarregado/UFU, dentro da Plataforma Fala.BR e este instruirá um Processo SEI para tratar da manifestação.

Caso não haja informações suficientes para a caracterização completa do incidente de segurança, o Encarregado poderá solicitar as informações complementares à pessoa manifestante. Se optar por registrar o incidente como denúncia anônima, a pessoa demandante deverá fazer o registro da maneira mais completa possível, pois não caberá solicitação de complementação, se necessária.

3.2 ANÁLISE DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

O Encarregado/UFU analisará a criticidade do incidente de segurança 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, dentre outras informações necessárias, no prazo de três dias úteis, conforme estabelecido na Resolução CD/ANPD N.º 15, de 24 de abril de 2024.

O Encarregado poderá contar com a colaboração de setores institucionais que tratem dos respectivos dados pessoais, e esses atuarão na complementação da análise, de forma técnica, subsidiando a confirmação ou não do incidente de segurança, sua extensão, a natureza dos dados afetados e riscos diversos. Após a eventual análise requerida pelo Encarregado, o setor deverá restituir o Processo SEI ao Encarregado, dentro do prazo mencionado acima, na forma de Despacho.

Caso se configure o incidente de segurança com dados pessoais, o Encarregado procederá, imediatamente, a comunicação à Agência Nacional de Proteção de Dados (ANPD), conforme instruções detalhadas no Item 4 deste Guia, bem como ao titular, conforme o Item 5.

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

Caso seja confirmada a necessidade de comunicação do incidente de segurança à Agência Nacional de Proteção de Dados (ANPD) - Item 3 deste Guia, o Encarregado LGPD/UFU deverá procedê-lo conforme orientações disponíveis no site "**Comunicação de incidente de segurança - Agência Nacional de Proteção de Dados**" (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis), por meio de formulário eletrônico disponibilizado pela ANPD ("**Formulário de Comunicação de Incidente à ANPD**"), no prazo de três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. Essa comunicação conterá as seguintes informações (§ 2º, Art. 6º, Resolução CD/ANPD Nº 15/2024):

- 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 determiná-la, e a de seu conhecimento pelo controlador;
- VIII - os dados do encarregado ou de quem represente o controlador;
- IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;
- X - a identificação do operador, quando aplicável;
- XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

As informações listadas acima poderão ser complementadas, de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação à ANPD (§ 3º, Art. 6º, Resolução CD/ANPD Nº 15/2024).

Nos casos que tratem de informações cujo sigilo seja protegido por lei, como dados e informações técnicas, econômico-financeiras, contábeis, operacionais, cuja divulgação possa representar violação a segredo comercial ou a industrial, o Encarregado LGPD/UFU, em nome da Universidade Federal de Uberlândia, deverá solicitar à ANPD de maneira fundamentada o respectivo sigilo, indicando aqueles dados/informações cujo acesso deverá ser restringido, em observância ao Art. 7º da Resolução CD/ANPD Nº 15/2024.

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.

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

Caso seja confirmada a necessidade de comunicação do incidente de segurança (Item 3 deste Guia), o Encarregado LGPD/UFU deverá procedê-lo junto ao titular, também, no prazo de três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. Essa comunicação conterá as seguintes informações (Art. 9º, Resolução CD/ANPD Nº 15/2024):

- 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 devido;
- 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.

Em cumprimento ao estabelecido pelo Art. 9º, o Encarregado/UFU fará essa comunicação com linguagem simples e de fácil entendimento, e de forma direta e individualizada, por meio de e-mail, contato telefônico ou mesmo carta, caso seja possível identificar o titular. Porém, se a comunicação direta e individualizada se mostre inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, o Encarregado/UFU fará a comunicação do incidente pelos canais institucionais, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

O Encarregado/UFU juntará ao processo SEI de registro do incidente, uma declaração de que foi realizada a comunicação ao titular, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo inicialmente estabelecido de três dias úteis (§ 4º, Art. 9º, Resolução CD/ANPD Nº 15/2024).

Ainda, em observância ao disposto no Art. 9º em referência, 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.

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

A Universidade Federal de Uberlândia, enquanto controladora, nos termos do Art. 10 da Resolução CD/ANPD Nº 15/2024, manterá o registro dos incidentes de segurança, inclusive dos não comunicados à ANPD e aos titulares, pelo prazo de cinco anos, contado a partir da data de registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

O registro do incidente será feito pelo Encarregado/UFU, por meio do "**Formulário de Registro de Incidente de Segurança pelo Encarregado**" (**Anexo II** deste Guia), em Processo SEI, que deverá conter, no mínimo (§ 2º, Art. 10, Resolução CD/ANPD Nº 15/2024):

- 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.

7. DISPOSIÇÕES FINAIS

Havendo a necessidade de revisão e atualização do presente Guia, a proposta poderá ser formulada e apresentada pela Comissão de Análise e Implementação da Lei Geral de Proteção de Dados Pessoais na Universidade Federal de Uberlândia - CLGPD/UFU à apreciação e deliberação por parte do Comitê de Governança Digital da Universidade Federal de Uberlândia CGD/UFU.

8. REFERÊNCIAS

BRASIL. Agência Nacional de Proteção de dados. **Comunicação de incidentes de segurança**. Disponível em: < <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca> >. Acesso em: 20 de janeiro de 2026.

BRASIL. Agência Nacional de Proteção de dados. **Regulamento de Comunicação de incidentes de segurança**. Disponível em: < <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024> >. Acesso em: 20 de janeiro de 2026.

BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 20 de janeiro de 2026.

ANEXO I

Formulário de Notificação de Incidente de Segurança ao Encarregado

1. Identificação da Pessoa Comunicante	
Nome Completo	Clique ou toque aqui para inserir o texto.
Unidade / Lotação	Clique ou toque aqui para inserir o texto.
E-mail de Contato	Clique ou toque aqui para inserir o texto.
Telefone para Contato	Clique ou toque aqui para inserir o texto.
Data de Comunicação	Clique ou toque aqui para inserir o texto.

2. Descrição Geral do Incidente	
Data e Hora de Ocorrência do Incidente (ou da suspeita)	Clique ou toque aqui para inserir o texto.
Data e Hora da Ciência do Incidente (quando você soube)	Clique ou toque aqui para inserir o texto.
Descrição do Incidente (descreva objetivamente o que ocorreu, como descobriu, em que meio, se há envolvido, e qual a localização física ou lógica dos dados afetados)	Clique ou toque aqui para inserir o texto.
Descrição da Causa Principal do Incidente (se identificada)	Clique ou toque aqui para inserir o texto.

3. Dados Pessoais Afetados	
Natureza dos Dados Pessoais Afetados	☐ Dados Pessoais Gerais ☐ Dados Pessoais Sensíveis ☐ origem racial ou étnica ☐ convicção religiosa ☐ opinião política ☐ filiação a sindicato ou a organização de caráter religioso, filosófico ou político ☐ referente à saúde ☐ referente à vida sexual ☐ dado genético ou biométrico
Categoria dos Dados Pessoais Afetados	☐ Dados de Crianças, de Adolescentes ou de Idosos ☐ Dados Financeiros ☐ Dados de Autenticação em Sistemas ☐ Dados Protegidos por Sigilo Legal, Judicial ou Profissional ☐ Dados em Larga Escala
Número de Titulares Afetados (total e, se aplicável, número de Crianças, Adolescentes e/ou Idosos)	Clique ou toque aqui para inserir o texto.
Tipo de Violação (marque as principais suspeitas)	☐ Acesso não Autorizado ☐ Vazamento / Comunicação Indevida ☐ Alteração Indevida ☐ Perda / Destruição ☐ Sequestro de Dados (<i>Ransomware</i>) ☐ Roubo / Furto de Equipamento ☐ Outra (especifique): Clique ou toque aqui para inserir o texto.

ANEXO II

Formulário de Registro de Incidente de Segurança pelo Encarregado

1. Descrição Geral do Incidente	
Data de Conhecimento do Incidente	Clique ou toque aqui para inserir o texto.
Descrição Geral das Circunstâncias em que o Incidente ocorreu	Clique ou toque aqui para inserir o texto.
Outras Informações Relevantes	Clique ou toque aqui para inserir o texto.

2. Dados Pessoais Afetados	
Natureza dos Dados Pessoais Afetados	☐ Dados Pessoais Gerais ☐ Dados Pessoais Sensíveis ☐ origem racial ou étnica ☐ convicção religiosa ☐ opinião política ☐ filiação a sindicato ou a organização de caráter religioso, filosófico ou político ☐ referente à saúde ☐ referente à vida sexual ☐ dado genético ou biométrico
Categoria dos Dados Pessoais Afetados	☐ Dados de Crianças, de Adolescentes ou de Idosos ☐ Dados Financeiros ☐ Dados de Autenticação em Sistemas ☐ Dados Protegidos por Sigilo Legal, Judicial ou Profissional ☐ Dados em Larga Escala
Avaliação do Risco	Clique ou toque aqui para inserir o texto.
Possíveis Danos aos Titulares	Clique ou toque aqui para inserir o texto.

3. Ações Corretivas e Mitigadoras (quando aplicáveis)	
Medidas de Correção	Clique ou toque aqui para inserir o texto.
Medidas de Mitigação	Clique ou toque aqui para inserir o texto.

4. Comunicação do Incidente de Segurança	
Forma e Conteúdo da Comunicação à ANPD	Clique ou toque aqui para inserir o texto.
Forma e Conteúdo da Comunicação aos Titulares	Clique ou toque aqui para inserir o texto.
Motivo de Ausência de Comunicação (quando for o caso)	Clique ou toque aqui para inserir o texto.