LGPD

Guia para comunicação de incidentes de segurança com dados pessoais para agentes públicos do MIDR

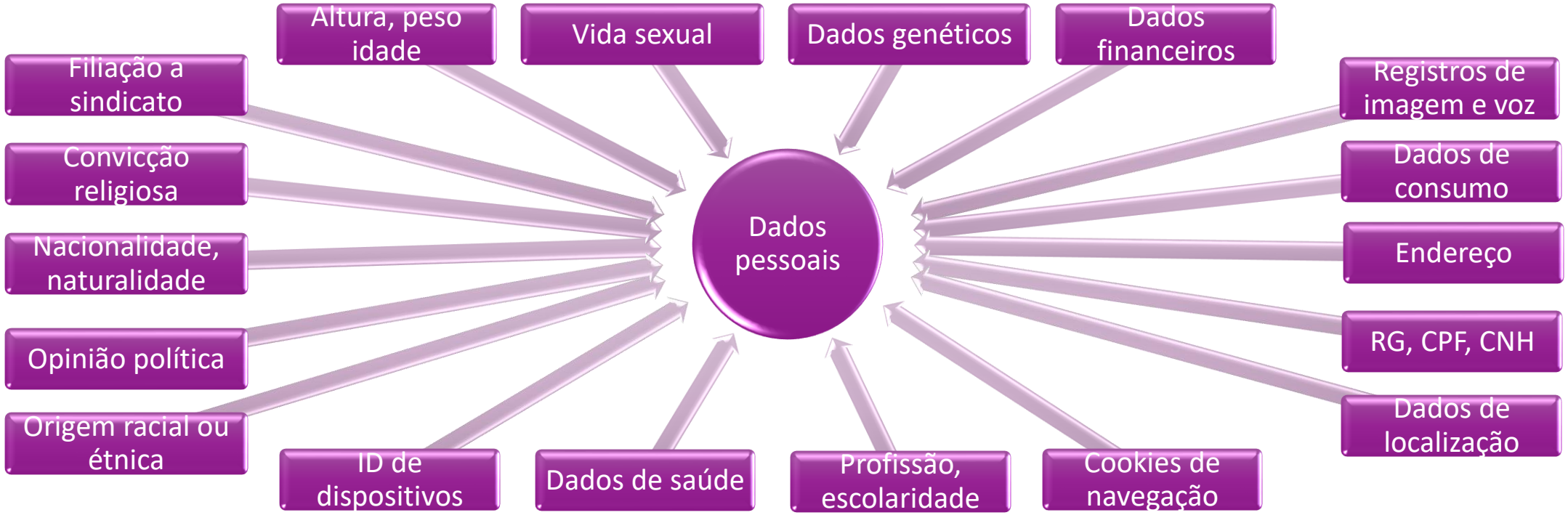
COMITÊ DE GOVERNANÇA DIGITAL, SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS - CGDSP

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

OBJETIVO

Este Guia tem como objetivo orientar os servidores e colaboradores do Ministério da Integração e do Desenvolvimento Regional (MIDR) sobre os procedimentos a serem adotados em caso de suspeita ou constatação de ocorrência de incidente de segurança que envolva dados pessoais.



O QUE É UM INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS?

Considera-se incidente de segurança com dados pessoais qualquer evento, seja ele acidental ou ilícito, que possa comprometer a segurança, a confidencialidade, integridade ou disponibilidade desses dados.

- Perda, destruição ou indisponibilidade dos dados
- Vazamento de informações
- Acesso indevido
- Roubo, extravio ou perda de equipamento com dados pessoais
- Exclusão ou alteração indevida
- Envio de dados pessoais ao destinatário errado
- Captura de credencial
- Publicação ou disponibilização indevida de dados pessoais
- Falha na segurança de sistema
- Abandono de documento em impressora
- Fraude ou erro de certificação de identidade
- Erro de registro ou cadastro
- Informação desatualizada ou incompleto
- Tratamento não informado ou acordado com o titular

QUEM DEVE COMUNICAR INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS NO MIDR?

Todo servidor e colaborador do Ministério da Integração e do Desenvolvimento Regional (MIDR) que tenha ciência ou suspeita de um incidente de segurança envolvendo dados de pessoas físicas tratados na Pasta deve informar o fato, imediatamente à Equipe de Prevenção, Tecnologia e Resposta a Incidentes (ETIR), ou solicitar a sua chefia imediata que o faça.

A comunicação à ETIR deve ser feita por um dos seguintes canais:

- Sistema Eletrônico de Informações (SEI), unidade "ETIR";
- E-mail: etir@mdr.gov.br; ou
- Telefone: (61) 2034-5890.

RESPONSABILIDADES DA EQUIPE DE PREVENÇÃO, TECNOLOGIA E RESPOSTA A INCIDENTES CIBERNÉTICOS

A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), da Diretoria de Tecnologia da Informação do MIDR, foi instituída com o objetivo de garantir a segurança, a integridade e a confidencialidade das informações tratadas pelos sistemas informatizados da Pasta.

Ao receber a comunicação de um incidente, a ETIR deverá:

1) Avaliar o tipo, a quantidade de dados pessoais afetados e os possíveis impactos para os titulares;

2) Caso seja identificado risco ou dano relevante aos titulares, comunicar o responsável pela gestão dos dados e o Encarregado, por meio do "Formulário de Comunicação de Incidente (LGPD)", em processo SEI do tipo "LGPD - Comunicação de Incidente de Segurança", mantendo-os informados sobre a evolução das ações, até a restauração da normalidade.

3) Caso o incidente seja considerado de maior impacto, comunicar o Centro Integrado de Segurança Cibernética do Governo Digital (CISC) e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), mantendo-os informados sobre a evolução das ações, até a normalização.

RESPONSABILIDADES DOS GESTORES RESPONSÁVEIS PELO TRATAMENTO DOS DADOS PESSOAIS

Em caso de suspeita ou constatação de incidente, os gestores responsáveis pelo tratamento dos dados pessoais deverão adotar as seguintes providências:

1) Formalizar comunicação à ETIR;

2) Avaliar, em conjunto com o Encarregado e a ETIR, a necessidade e a forma de comunicação do incidente aos titulares dos dados pessoais afetados;

3) Realizar a comunicação do incidente aos titulares de dados afetados;

4) Acompanhar e colaborar com a ETIR, na adoção das medidas de resposta ao incidente, mantendo os titulares informados, até que a normalidade seja restaurada.

RESPONSABILIDADES DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

No MIDR, compete à Ouvidoria exercer a função de Encarregado pelo Tratamento de Dados Pessoais, nos termos do art. 41 da Lei nº 13.709/2018 (LGPD).

Ao receber o "Formulário de Comunicação de Incidente (LGPD)", com a informação de risco ou dano relevante causado aos titulares de dados pessoais, o Encarregado deverá adotar as seguintes ações:

1) Apoiar os gestores responsáveis pelo tratamento dos dados pessoais na definição da forma e do conteúdo da comunicação do incidente aos titulares de dados;

2) Realizar a comunicação à Agência Nacional de Proteção de Dados (ANPD), bem como promover o atendimento a suas recomendações;

3) Acompanhar as medidas de resposta ao incidente, mantendo a ANPD atualizada sobre a evolução das ações de mitigação dos impactos decorrentes, até o retorno à normalidade, quando a comunicação formal for aplicável.

QUANDO O ENCARREGADO VAI COMUNICAR O INCIDENTE À ANPD?

De acordo com o art. 5º da Resolução CD/ANPD nº 15, de 24 de abril de 2024, o incidente de segurança deve ser comunicado à ANPD quando puder acarretar risco ou dano relevante ao titular, como:

- impedir o exercício de direitos ou a utilização de um serviço
- ocasionar danos materiais ou morais (discriminação, violação à integridade física, ao direito à imagem e à reputação)
- fraudes financeiras ou roubo de identidade

Além disso, o incidente também deve envolver pelo menos um dos seguintes critérios:

- dados pessoais sensíveis
- 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

SUSPEITA OU CONSTATAÇÃO DE ILEGALIDADE OU IRREGULARIDADE

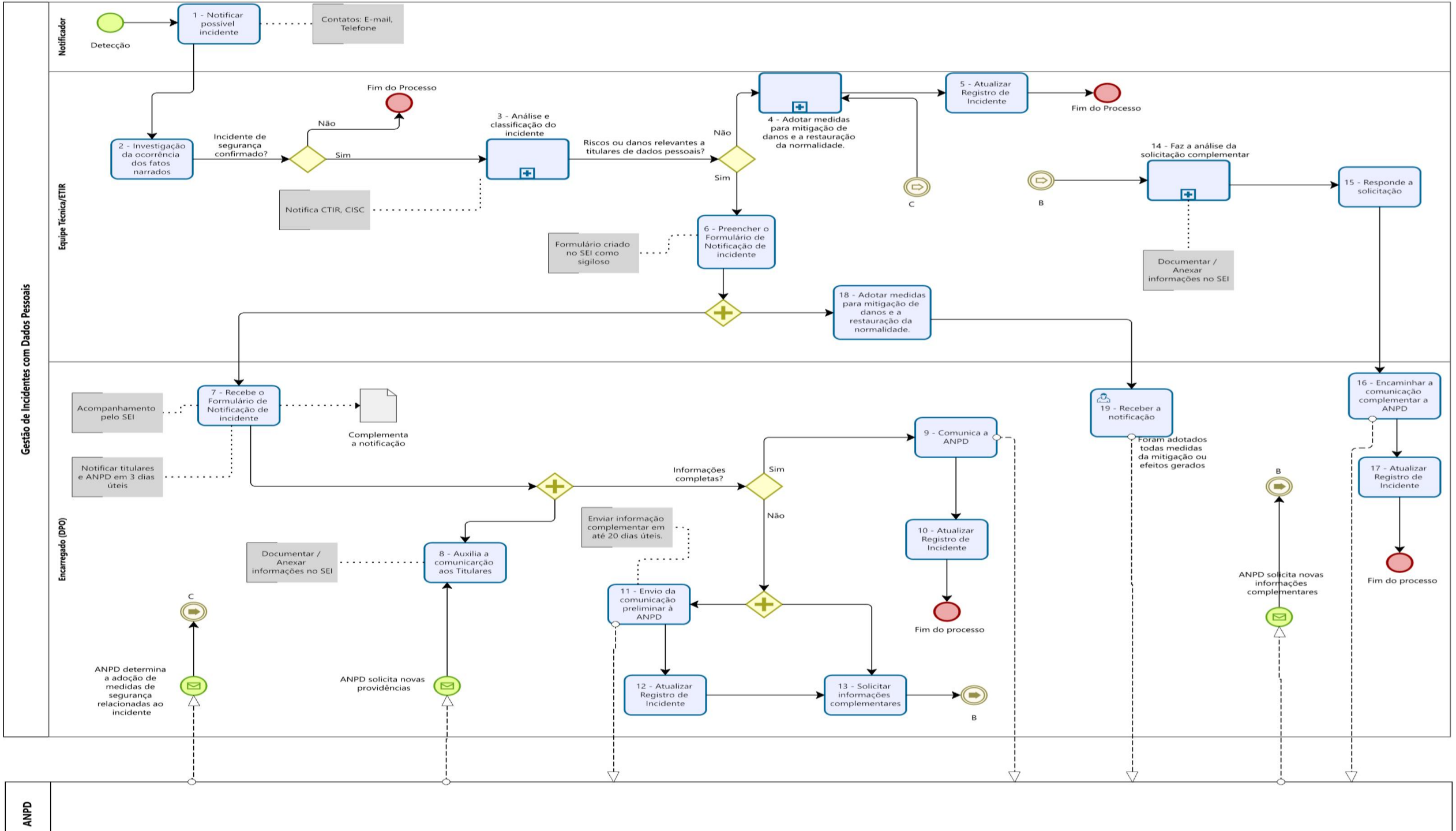
Em caso de suspeita ou constatação de irregularidade ou ilegalidade no tratamento de dados pessoais, o agente público deverá registrar representação, por meio de processo sigiloso no SEI, a ser encaminhada:

- ao titular da Assessoria Especial de Controle Interno (AECI), quando houver indícios de crime cibernético, para a adoção das providências necessárias junto aos órgãos de controle e segurança competentes; e
- ao titular da Corregedoria, em caso de indícios de infração disciplinar praticada por servidor público.

As denúncias e comunicações anônimas de ilegalidades ou irregularidades no tratamento de dados pessoais deverão ser encaminhadas à Ouvidoria do MIDR, por meio da plataforma Fala.Br.

A instrução de representações e denúncias deverá conter o maior número possível de informações disponíveis, a fim de subsidiar a adequada apuração dos fatos:

quem praticou a irregularidade ou ilegalidade	descrição dos atos praticados	identificação dos locais e meios utilizados	descrição da forma como o fato aconteceu	indicação da data e da hora em que aconteceu	identificação dos motivos que podem ter levado à prática do ato


Gestão de Incidentes com Dados Pessoais
Notificador
Equipe Técnica/ETIR
Encarregado (DPO)
ANPD
Detecção
1 - Notificar possível incidente
Contatos: E-mail, Telefone
2 - Investigação da ocorrência dos fatos narrados
Incidente de segurança confirmado?
Não
Sim
Fim do Processo
Notifica CTIR, CISC
3 - Análise e classificação do incidente
Riscos ou danos relevantes a titulares de dados pessoais?
Não
Sim
4 - Adotar medidas para mitigação de danos e a restauração da normalidade.
5 - Atualizar Registro de Incidente
Fim do Processo
C
B
14 - Faz a análise da solicitação complementar
Documentar / Anexar informações no SEI
15 - Responde a solicitação
6 - Preencher o Formulário de Notificação de incidente
Formulário criado no SEI como sigiloso
18 - Adotar medidas para mitigação de danos e a restauração da normalidade.
7 - Recebe o Formulário de Notificação de incidente
Acompanhamento pelo SEI
Complementa a notificação
Notificar titulares e ANPD em 3 dias úteis
Informações completas?
Sim
Não
9 - Comunica a ANPD
10 - Atualizar Registro de Incidente
Fim do processo
Enviar informação complementar em até 20 dias úteis.
11 - Envio da comunicação preliminar à ANPD
12 - Atualizar Registro de Incidente
13 - Solicitar informações complementares
B
8 - Auxilia a comunicarção aos Titulares
Documentar / Anexar informações no SEI
ANPD solicita novas providências
C
ANPD determina a adoção de medidas de segurança relacionadas ao incidente
19 - Receber a notificação
Foram adotados todas medidas da mitigação ou efeitos gerados
16 - Encaminhar a comunicação complementar a ANPD
17 - Atualizar Registro de Incidente
Fim do processo
B
ANPD solicita novas informações complementares

LGPD

MINISTÉRIO DA
INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO