



Plano de Resposta a Incidentes de Segurança



Governador do Estado
Jorginho dos Santos Mello

Secretário de Estado da Agricultura
Admir Edi Dalla Cort

Presidente da Epagri
Dirceu Leite

Diretores

Andréia Meira
Ensino Agrotécnico

Jurandi Teodoro Gugel
Desenvolvimento Institucional

Fabírcia Hoffmann Maria
Administração e Finanças

Gustavo Gimi Santos Claudino
Extensão Rural e Pesqueira

Everton Blainski
Ciência, Tecnologia e Inovação



Plano de Resposta a Incidentes de Segurança



**Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina
Florianópolis
2026**

Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina (Epagri)
Rodovia Admar Gonzaga, 1.347, Itacorubi, Caixa Postal 502
88034-901, Florianópolis, Santa Catarina, Brasil
Fone: (48) 3665-5000
Site: www.Epagri.sc.gov.br

Editado pelo Departamento Estadual de Marketing e Comunicação (Epagri/DEMC)

Aprovado conforme a 21ª Ata da Reunião da Diretoria Executiva, do dia 30/06/2026.

Equipe técnica de elaboração:

Natália Junqueira Carvalho Costa (Encarregada de Dados Pessoais da Epagri).

José Pedro Oliveira Rosses (Controlador Interno e Ouvidor)

Augusto Ferreira de Souza (Gestor do DEGTI)

Editoração técnica: João Vieira Neto

Revisão: Laertes Rebelo e Maria Luíza Chaves

Diagramação: Vilton Jorge de Souza

Distribuição: *on-line*

Primeira edição: agosto 2026

É permitida a reprodução parcial deste trabalho desde que a fonte seja citada.

Ficha catalográfica

S231p	Santa Catarina. Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina. Plano de resposta a incidentes de segurança. – Florianópolis: Epagri, 2026. 34 p.; – (Regimentos e Normas). 1. Segurança da Informação. 2. Proteção de Dados. 3. Medidas de segurança. 4. Epagri. I. Título. CDD: 005.8
-------	---

Elaborado por: Bibliotecária Rafaela Rocha Rabelo - CRB 14/1934

APRESENTAÇÃO

O Plano de Resposta a Incidentes de Segurança da Epagri estabelece as diretrizes, responsabilidades e procedimentos para a identificação, tratamento e mitigação de incidentes que possam comprometer a segurança da informação no âmbito da Empresa. Este documento complementa a Política de Segurança da Informação (POSIN), alinhando-se à Lei Geral de Proteção de Dados Pessoais (LGPD), à [Resolução CD/ANPD nº 15/2024](#) e às boas práticas de governança em segurança da informação adotadas pela Administração Pública.

Trata-se de um instrumento normativo essencial para garantir a pronta resposta a eventos adversos e visa minimizar impactos operacionais, institucionais e reputacionais, bem como assegurar a proteção dos dados pessoais e das informações estratégicas sob responsabilidade da Epagri.

O plano define fluxos claros de atuação e promove a integração entre áreas técnicas, administrativas e de governança, de forma a assegurar tratamento adequado, tempestivo e auditável dos incidentes. Sua aplicação orienta a atuação de usuários, prestadores de serviço e demais agentes envolvidos. Além de fortalecer a cultura de segurança da informação e de proteção de dados pessoais na Empresa, tem como objetivo contribuir para a melhoria contínua dos processos institucionais.

Aprovado pela Diretoria Executiva, este plano reflete o compromisso da Epagri com a integridade, a confidencialidade e a disponibilidade das informações, bem como com a transparência, a conformidade legal e a gestão responsável de incidentes de segurança envolvendo dados pessoais.

A Diretoria Executiva

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Agência Nacional de Proteção de Dados

CIASC – Centro de Informática e Automação do Estado de Santa Catarina S.A

CIS – Comunicação de Incidente de Segurança

DEGTI – Departamento Estadual de Gestão de Tecnologia da Informação

DEGOP – Departamento Estadual de Gestão Operacional

DEGP – Departamento Estadual de Gestão de Pessoas

DEMC – Departamento Estadual de Marketing e Comunicação

DJUR – Departamento Jurídico

DPO – Encarregado de Dados (*Data Protection Officer*)

IDP – Inventário de Dados Pessoais

IDS/IPS – Sistemas de Prevenção e Detecção de Intrusão (*Intrusion Detection System/ Intrusion Prevention System*)

LGPD – Lei Geral de Proteção de Dados Pessoais

NTP – *Network Time Protocol*

POSIN – Política de Segurança da Informação

RIPD – Relatório de Impacto à Proteção de Dados Pessoais

SEA/SC – Secretaria de Estado da Administração de Santa Catarina

SGP-e – Sistema de Gestão de Processos Eletrônicos

TCE/SC – Tribunal de Contas do Estado de Santa Catarina

LISTA DE FIGURAS

Figura 1 - Ciclo de Resposta a Incidentes de Segurança da Informação

Figura 2 - Ciclo de Resposta a Incidentes de Segurança com Dados Pessoais

Figura 3 - Medidas de segurança

Figura 4 - Comunicação à ANPD

Figura 5 - Ciclo PDCA

LISTA DE QUADROS

Quadro 1 - Fluxo de Incidentes de Segurança

Quadro 2 - Responsabilidade da Triagem

Quadro 3 - Matriz de Impacto

Sumário

APRESENTAÇÃO	3
1 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA.....	7
2 OBJETIVOS.....	7
2.1 Campo de aplicação e escopo	8
3 INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS.....	8
4 CLASSIFICAÇÃO E FLUXO DOS INCIDENTES DE SEGURANÇA.....	8
4.1 Fluxo de Incidentes de Segurança	9
5 RESPONSABILIDADES E CICLOS DE RESPOSTA A INCIDENTES DE SEGURANÇA	9
5.1 Usuário	9
5.2 Gestor da Unidade.....	10
5.3 Departamento Estadual de Gestão de Tecnologia da Informação (DEGTI).....	10
5.4 Encarregado de Dados (DPO)	10
5.5 Ouvidoria	10
5.6 Controle interno	11
5.7 Outros departamentos	11
5.8 Equipe para Tratamento de Incidentes de Maior Complexidade	11
5.9 Ciclo de Resposta a Incidentes de Segurança da Informação	11
5.10 Ciclo de Resposta a Incidentes de Segurança com Dados Pessoais.....	12
6 DETECÇÃO E NOTIFICAÇÃO DO INCIDENTE DE SEGURANÇA	13
6.1 Incidentes não digitais.....	14
7 TRIAGEM E ANÁLISE INICIAL DO IMPACTO	14
7.1 Informações iniciais.....	15
7.2 Deveres específicos do Operador de Dados Pessoais.....	15
7.3 Informações complementares.....	15

7.4 Envolvimento multidepartamental.....	17
8 REGISTRO INTERNO DO INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS	18
8.1 Procedimentos de Registro no SGP-e	19
8.2 Conteúdo Mínimo do Registro	20
8.3 Fluxo de tramitação.....	20
9 CONTENÇÃO E ERRADICAÇÃO DO INCIDENTE DE SEGURANÇA	21
9.1 Avaliação Técnica e Funcional	21
9.2 Medidas de Contenção e Erradicação (Meios Digitais)	22
9.3 Medidas de Contenção e Erradicação (Meios Não Digitais/Físicos)	22
10 RECUPERAÇÃO	23
11 COMUNICAÇÕES À ANPD E AO TITULAR DE DADOS PESSOAIS	24
11.1 Prazos e Responsabilidades.....	25
11.2 Comunicações do Incidente ao Titular de Dados	25
11.3 Relatório do Incidente à ANPD	26
11.4 Padronização de resposta.....	26
12 ADEQUAÇÃO E MELHORIA CONTÍNUA.....	27
12.1 Diretrizes gerais	27
12.2 Metodologia de Melhoria Contínua	28
12.3 Monitoramento e indicadores.....	28
12.4 Reuniões de lições aprendidas	28
13 RELATÓRIO DE TRATAMENTO DE INCIDENTE	29
14 ENCERRAMENTO FORMAL DO INCIDENTE.....	29
15 SENSIBILIZAÇÃO DOS FUNCIONÁRIOS E REVISÃO DO PLANO.....	30
16 FLUXO – CADEIA DE VALOR.....	30
17 GLOSSÁRIO	30
18 REFERÊNCIAS.....	34

1 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Este Plano de Resposta a Incidentes de Segurança foi elaborado com base no guia utilizado pelo Governo Federal, constituindo-se como um complemento aos demais planos da Política de Segurança da Informação da Epagri.

Esta Norma de Procedimento estabelece diretrizes, responsabilidades e procedimentos para a gestão de incidentes de segurança da informação no âmbito da Epagri, com ênfase nos incidentes que envolvam dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), a Resolução CD/ANPD nº 15/2024, e demais normativos aplicáveis.

Este Plano poderá ser complementado por fluxogramas, instruções de trabalho e orientações técnicas emitidas pelo Encarregado de Dados, de acordo com a LGPD e normas emitidas pela ANPD.

2 OBJETIVOS

Com a implementação deste Plano de Resposta a Incidentes, pretende-se alcançar os seguintes objetivos:

- Orientar a resposta a incidentes de segurança estabelecendo procedimentos documentados, formais, rápidos, confiáveis e auditáveis;
- Definir claramente os fluxos de procedimentos e responsabilidades institucionais;
- Minimizar impactos operacionais e preservar a reputação da Epagri;
- Assegurar conformidade com a LGPD e orientações da ANPD;
- Quantificar e monitorar o desempenho na proteção de dados pessoais;
- Promover a melhoria contínua com base nas lições aprendidas.

2.1 Campo de aplicação e escopo

Este Plano de Resposta a Incidentes de Segurança aplica-se a todas as unidades organizacionais da Epagri, abrangendo usuários, prestadores de serviço, operadores de dados e demais agentes que realizam tratamento de informações ou utilizam ativos institucionais. O escopo contempla incidentes de segurança da informação em meios digitais e não digitais, incluindo aqueles que envolvam dados pessoais, conforme a LGPD e os normativos aplicáveis, abrangendo eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações.

3 INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Todo incidente deve ser registrado internamente na Epagri, conforme o art. 10 da Resolução [CD/ANPD nº 15/2024](#). Entretanto, não é todo incidente que deve ser comunicado à Agência Nacional de Proteção de Dados – ANPD.

Orientações da ANPD: todas as notificações, independentemente do grau de risco ou impacto, devem ser registradas.

4 CLASSIFICAÇÃO E FLUXO DOS INCIDENTES DE SEGURANÇA

Os incidentes deverão ser classificados em:

- **Incidente de Segurança da Informação**

Eventos que não envolvem dados pessoais ou que não apresentam impacto relevante à privacidade.

- **Incidente de Segurança com Dados Pessoais**

Eventos que envolvem dados pessoais e demandam avaliação conforme LGPD e normativos da ANPD.

4.1 Fluxo de Incidentes de Segurança

Quadro 1 - Fluxo de Incidentes de Segurança

Atividade	Incidente de Segurança da Informação - Digital	Incidente de Segurança com Dados Pessoais
Prazo de Triagem	Imediato (máximo de 24h)	Imediato (máximo de 24h)
Registro Interno	Opcional (Sistemas de chamado do DEGTI e Relatórios para Melhoria Contínua)	Obrigatório para auditoria da ANPD (SGP-e)
Comunicação Externa	Caso necessário	Obrigatória (em certos casos)
Prazo de Notificação	Não existe	Máximo de 3 dias úteis
Responsável Prioritário	DEGTI (conforme a natureza do Incidente)	DPO (conforme a natureza do Incidente)

Fonte: Elaborado pelo autor (2026).

Diretrizes gerais

As unidades envolvidas no incidente e demais departamentos citados no item 7.3, quando for o caso, deverão fornecer suporte imediato e contínuo.

A unidade envolvida no incidente e o DEGTI deverão cientificar imediatamente o DPO quando houver dúvida quanto ao envolvimento de dados pessoais.

Os incidentes físicos/não digitais e sem envolvimento de dados pessoais seguem rito simplificado sob responsabilidade do Gestor da Unidade, conforme item 6.1.

5 RESPONSABILIDADES E CICLOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

5.1 Usuário

- Detectar e identificar possíveis incidentes de segurança da informação;
- Comunicar imediatamente o superior hierárquico e o Gestor da Unidade sobre qualquer incidente de segurança;
- Colaborar com o Gestor no fornecimento das informações necessárias para o preenchimento do registro inicial;

- d) Preservar evidências do incidente, evitando a manipulação indevida de arquivos ou sistemas afetados até a orientação da equipe técnica;
- e) Colaborar com o DPO e o DEGTI na prestação de informações complementares e seguir rigorosamente as instruções de contenção recebidas.

5.2 Gestor da Unidade

- a) Receber do usuário a comunicação inicial do incidente;
- b) Avaliar preliminarmente a situação para fornecer os dados primários de triagem;
- c) Preencher o Formulário de Comunicação Interna de Incidente de Segurança;
- d) Acionar as áreas competentes conforme a natureza do incidente;
- e) Acompanhar o tratamento do incidente na unidade;
- f) Apoiar o usuário para preservar evidências do incidente e colaborar com o DPO e o DEGTI na prestação de informações complementares.

5.3 Departamento Estadual de Gestão de Tecnologia da Informação (DEGTI)

- a) Realizar a análise técnica dos incidentes que envolvam sistemas de informação;
- b) Executar ações de contenção, mitigação e recuperação técnica;
- c) Preservar evidências digitais;
- d) Apoiar a análise do incidente.

5.4 Encarregado de Dados (DPO)

- a) Avaliar incidentes que envolvam ou possam envolver dados pessoais;
- b) Orientar quanto à aplicação da LGPD;
- c) Decidir sobre a necessidade de comunicação à ANPD e aos titulares;
- d) Acompanhar o tratamento dos incidentes com dados pessoais.

5.5 Ouvidoria

- a) Encaminhar ao DPO todas as manifestações (denúncias, solicitações etc.) ou pedidos de acesso à informação apresentados por titulares de dados à Ouvidoria que envolvam o exercício de direitos previstos no art. 18 da LGPD ou por terceiros relacionados a incidentes de segurança da informação, para análise, adoção das providências cabíveis e elaboração de resposta ao titular;
- b) Direcionar às áreas competentes denúncias de outras naturezas.

5.6 Controle interno

- a) Acompanhar, quando aplicável, os incidentes de segurança da informação, especialmente aqueles de natureza administrativa ou não digital;
- b) Acompanhar a apuração de eventuais falhas de processo, irregularidades ou responsabilidades administrativas;
- c) Propor recomendações para aprimoramento dos controles internos e mitigação de riscos operacionais, financeiros e de conformidade, sem prejuízo da atuação do DPO;
- d) Apoiar as ações da Auditoria Interna e demais órgãos de controle relacionadas aos incidentes.

5.7 Outros departamentos

A critério do responsável pela avaliação do incidente, poderão ser acionados outros departamentos para apoio.

5.8 Equipe para Tratamento de Incidentes de Maior Complexidade

Poderá ser constituída, a critério da gestão, equipe específica para tratamento de incidentes de maior complexidade, com participação das áreas técnicas e administrativas envolvidas, especialmente quando houver impacto relevante, risco institucional ou necessidade de atuação multidisciplinar.

5.9 Ciclo de Resposta a Incidentes de Segurança da Informação

Aplica-se aos incidentes que não envolvam dados pessoais ou que não apresentem impacto relevante à privacidade.

Figura 1 – Ciclo de Resposta a Incidentes de Segurança da Informação



Fonte: Elaborado pelo autor (2026).

5.10 Ciclo de Resposta a Incidentes de Segurança com Dados Pessoais

Aplica-se aos incidentes que envolvam dados pessoais ou que apresentem impacto relevante à privacidade.

Figura 2 – Ciclo de Resposta a Incidentes de Segurança com Dados Pessoais



Fonte: Elaborado pelo autor (2026).

6 DETECÇÃO E NOTIFICAÇÃO DO INCIDENTE DE SEGURANÇA

Detecção:

- DEG TI: medidas técnicas de detecção;
- Usuários da Epagri;
- Operador de dados, contratante ou contratado;
- Titular de Dados;
- Sociedade.

Canais de notificação:

- **Comunicação Interna** através do [Formulário de Comunicação Interna de Incidente](#);
- **Comunicação Externa** através do [Formulário de Comunicação Externa de Incidente de Segurança - Operador de Dados](#);
- **Canal Oficial da LGPD no Poder Executivo Estadual** - <https://www.sc.gov.br/servicos/solicitar-atendimento-lgpd>: titular de dados e sociedade.
- **Ouvidoria da Epagri** - (<https://www.epagri.sc.gov.br/ouvidoria/>): titular de dados e sociedade;
- Outros canais: Departamento Estadual de Gestão da Tecnologia de Informação (deg ti@epagri.sc.gov.br) e Encarregado de Dados Pessoais (dpo@epagri.sc.gov.br).



PRAZOS:

- **Operador de dados:** deve comunicar a Epagri **imediatamente** após a detecção de incidente, preenchendo o [Formulário](#) e encaminhando as informações técnicas preliminares no prazo estabelecido contratualmente.
- **Usuário (funcionário) da Epagri:** deve comunicar **imediatamente** o superior hierárquico/Gestor da Unidade, que será responsável por preencher o [Formulário](#) e acionar as áreas conforme a natureza do incidente:
 - DEG TI, nos casos que envolvam sistemas de informação;
 - Encarregado de Dados (DPO), nos casos que envolvam ou possam envolver dados pessoais.
- **Ouvidoria:** após receber manifestações (reclamações, denúncias, solicitações) ou pedido de acesso à informação sobre eventual incidente, deve comunicar **imediatamente** o DEG TI, o DPO ou a unidade organizacional responsável, conforme o caso.
- Na hipótese de dúvida quanto à natureza do incidente, o DPO deverá ser acionado para avaliação.

6.1 Incidentes não digitais

Incidentes não digitais que não envolvam dados pessoais, sistemas de segurança da informação e que não apresentem risco relevante decorrente da ausência de ação imediata deverão ser tratados pelo Gestor da Unidade responsável, seguindo os trâmites regulares de comunicação interna, mediante registro por e-mail do setor envolvido, com cópia ao Controle Interno pelo endereço controleinterno@epagri.sc.gov.br.

Nesses casos, **não se aplica** o fluxo detalhado de resposta a incidentes previsto nesta norma. Eles deverão ser registrados de forma simplificada para fins de melhoria contínua dos controles internos da Empresa.

7 TRIAGEM E ANÁLISE INICIAL DO IMPACTO

Quadro 2 – Responsabilidade da Triagem

Tipo de Incidente	Quem recebe primeiro
Digital	Superior → DEG TI
LGPD	Superior → DPO
Físico / administrativo	Superior
Denúncia externa	Ouvidoria → encaminha

Fonte: elaborado pelo autor (2026).

Prazo máximo de 24 horas, a partir do conhecimento do incidente pela Epagri, para a triagem inicial de incidentes que envolvam dados pessoais, alinhado às boas práticas de segurança da informação.

7.1 Informações iniciais

Para garantir a agilidade, a padronização e o alerta tempestivo às equipes de resposta logo após a detecção de um evento adverso, a coleta das informações iniciais deverá ser realizada obrigatoriamente por meio dos Formulários de Comunicação de Incidente:

- Usuários (empregados da Epagri): [Comunicação Interna de Incidente](#); ou
- [Comunicação Externa de Incidente](#).

O responsável pelo recebimento e triagem conduzirá a análise inicial com o suporte dos demais setores e avaliará:

- a) Informações iniciais sobre o incidente: data e horário do ocorrido, breve descrição do incidente, qual o tipo de incidente;
- b) Se envolve ou não dados pessoais. Neste caso, acionará **imediatamente** o DPO;
- c) Sistemas impactados, danos aparentes e riscos de agravamento em caso de inércia.

Na hipótese de dúvida quanto à classificação do incidente, este deverá ser tratado como potencial incidente com dados pessoais até avaliação do Encarregado de Dados (DPO).

7.2 Deveres específicos do Operador de Dados Pessoais

- a) Preservar todas as evidências do incidente (como *logs*, medidas aplicadas, riscos para mitigação, entre outros);
- b) Comunicar a Epagri imediatamente após a detecção de incidente, utilizando, obrigatoriamente, o [Formulário de Comunicação Externa de Incidente de Segurança - Operador de Dados](#)
- c) Encaminhar todas as evidências preservadas e complementares ao e-mail oficial do Encarregado de Dados (dpo@epagri.sc.gov.br).

7.3 Informações complementares

Após acionado, o DPO analisará se o incidente envolve realmente dados pessoais e qual o seu possível impacto conforme a definição de risco (Quadro 3 – Matriz de Impacto).

Se envolver dados pessoais, a equipe da Epagri ou operador de dados deverá preservar imediatamente todas as evidências do incidente (conforme os procedimentos de preservação de evidências e cadeia de custódia descritos na seção 9.2), e o DPO buscará informações técnicas complementares:

- a) Origem;
- b) Categoria e quantidade de titulares de dados pessoais afetados;
- c) Categoria e quantidade de dados afetados;
- d) Consequências do incidente para os titulares e para a entidade, tais como: danos morais, engenharia social/fraudes, perda de acesso aos dados, roubo de identidade, exposição de dados protegidos por sigilo profissional/legal;
- e) Criticidade;
- f) Probabilidade;
- g) Medidas técnicas adotadas antes do incidente de segurança informadas pelo DEGTI, que será responsável por responder e detalhar, entre outros, os seguintes controles de segurança:

Figura 3 - Medidas de segurança

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/Pseudonimização.	☐	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.

Fonte: ANPD (2024).

Quadro 3 - Matriz de Impacto

Nível	Impacto	Definição do Risco
Alto	Grave	Incidente comum: afeta informações críticas, gera impacto negativo severo à Epagri Incidente com dados pessoais: envolve risco ou dano relevante aos titulares, afetando significativamente seus interesses ou direitos fundamentais, caracterizado por, entre outros, impedir o exercício de direitos ou a utilização de um serviço, ou ocasionar danos materiais ou morais, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. <u>E, cumulativamente</u>, envolver pelo menos um dos seguintes critérios: dados pessoais sensíveis; dados de crianças, adolescentes ou idosos; dados financeiros; dados de autenticação em sistemas; dados protegidos por sigilo legal, judicial ou profissional; ou dados em larga escala.

Nível	Impacto	Definição do Risco
Médio	Significativo	Incidente comum: afeta informações não críticas, sem impacto imediato à reputação da Epagri. Incidente com dados pessoais: envolve dados pessoais comuns que possam identificar o titular e afetar interesses e direitos fundamentais (ocasionando, entre outros, danos materiais ou morais, como discriminação, fraudes ou roubo de identidade, ou impedindo a utilização de um serviço), mas que não preencham os critérios cumulativos exigidos no Nível Alto.
Baixo	Mínimo	Incidente comum: possível incidente ou tentativa sem sucesso, afeta informações sem danos aparentes ou impacto à reputação da Epagri. Incidente com dados pessoais: o incidente está relacionado a dados pseudonimizados ou a dados pessoais comuns e não afeta significativamente interesses e direitos fundamentais dos titulares, não impedindo, entre outros, o exercício de direitos ou a utilização de um serviço, e que não possui a capacidade de ocasionar danos materiais ou morais (como discriminação, violação à integridade física, à imagem, à reputação, fraudes financeiras ou roubo de identidade).

Fonte: Elaborado pelo autor (2026).

A matriz de impacto deverá ser utilizada para classificação do incidente, priorização do tratamento e apoio à decisão quanto à comunicação à ANPD e aos titulares de dados pessoais, quando for o caso.

Além da Matriz de Impacto (Quadro 3), o DPO e o DEGTI deverão avaliar e classificar a Recuperabilidade do evento em um dos seguintes níveis para orientar a alocação de esforços:

- a) Regular: o tempo de recuperação é previsível com os recursos existentes;
- b) Suplementado: o tempo de recuperação é previsível, mas exige o empenho de recursos adicionais;
- c) Estendido: o tempo de recuperação é imprevisível, sendo necessários recursos adicionais e ajuda externa;
- d) Não Recuperável: a recuperação do incidente não é possível (ex: dados já expostos publicamente), demandando o início imediato de investigação e comunicação.

7.4 Envolvimento multidepartamental

A depender da classificação do incidente, o DEGTI e o DPO poderão acionar, conforme a natureza e a gravidade do incidente:

- a) Gestores das áreas afetadas: para suporte em incidentes ou avaliação de processos específicos;

- b) DEGTI: para suporte técnico em sistemas, contenção digital e análise de *logs*;
- c) DEGP e Gestores de Contratos (DEGOP): em eventos envolvendo falhas humanas de usuários ou terceirizados;
- d) DJUR: para assessoria jurídica e avaliação de sigilos legais e comunicação às autoridades policiais competentes (como a Polícia Civil ou Delegacia de Repressão a Crimes de Informática) sempre que houver indícios de materialidade de crimes cibernéticos (ex: ataques *hacker*, *ransomware* ou invasão de dispositivo prevista em lei);
- e) DEMC e Ouvidoria: para estratégias de comunicação com o público, sociedade e resposta direta aos cidadãos em geral.
- f) Unidades de Controle e Diretoria Executiva: em casos de risco Alto para fins de monitoramento e decisões estratégicas, respectivamente;
- g) Equipe para Tratamento de Incidentes de Maior Complexidade;
- h) Instâncias externas competentes: quando aplicável, poderão ser acionados órgãos responsáveis pela infraestrutura tecnológica envolvida, especialmente o Centro de Informática e Automação do Estado de Santa Catarina (CIASC), bem como fornecedores e operadores de dados.

8 REGISTRO INTERNO DO INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Todo incidente de segurança que envolva dados pessoais deve ser formalizado via SGP-e **imediatamente** após a triagem (até 24 horas após o conhecimento do evento). Este registro é **obrigatório** para fins de auditoria da ANPD e cumprimento do princípio da responsabilização.

A omissão, a falha no registro interno ou o atraso injustificado na comunicação externa (sujeita ao exíguo **prazo regulatório de 3 dias úteis**) configuram infrações graves. O **descumprimento** do Regulamento de Comunicação de Incidente de Segurança (Resolução CD/ANPD Nº 15/2024) **poderá ensejar a instauração de Processo Administrativo Sancionador contra a Epagri**, conforme a [Resolução CD/ANPD nº 1, de 28 de outubro de 2021](#).

Em caso de condenação, a Empresa estará sujeita às severas penalidades previstas no art. 52 da LGPD e no Regulamento de Dosimetria e Aplicação de Sanções Administrativas ([Resolução CD/ANPD nº 4/2023](#)).

A ocultação do incidente, a ausência de cooperação ou a falta de adoção rápida de medidas corretivas são consideradas circunstâncias agravantes que elevam drasticamente a dosimetria da pena, podendo classificar a infração como de **ato faltoso de natureza grave**.

As sanções aplicáveis incluem:

- A publicização da infração, gerando incalculável dano reputacional e de imagem da Epagri perante a sociedade;
- O bloqueio ou a eliminação das bases de dados pessoais afetadas;
- A suspensão parcial ou total do funcionamento do banco de dados por até 6 (seis) meses prorrogáveis, o que acarretaria a paralisação das atividades e sistemas operacionais da Epagri;
- A proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;
- A aplicação de multas simples ou diárias que podem atingir até 2% do faturamento, limitadas a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração, caso o incidente esteja relacionado à atuação da Epagri em regime de concorrência. Operacionalizando políticas públicas, a Epagri terá o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, ou seja, não estará sujeita às multas como forma de sanções.

Por fim, ressalta-se que o gestor ou usuário que, por ação, omissão ou negligência, der causa ao descumprimento dos prazos legais e das diretrizes deste Plano, expondo a Epagri a tais sanções, **poderá ser responsabilizado pessoal, civil e administrativamente pelos danos ocasionados à instituição.**

8.1 Procedimentos de Registro no SGP-e

Devem ser abertos **imediatamente** após a triagem para documentar toda a resposta, evidências e relatórios internos relacionados a incidentes com dados pessoais.

Classe: 1446 - Proteção de Dados Pessoais

Assunto 018 - Processo sobre Incidentes de
Segurança de Dados Pessoais.

Restrição de acesso: Usuários lotados em setores de tramitação do processo.

Quando houver necessidade de notificar a ANPD, deve ser aberto também o SGP-e Assunto 011 (Comunicação de Incidente à Autoridade Nacional de Proteção de Dados – ANPD), com caráter comprobatório e externo, devendo ser anexado o protocolo de comunicação à ANPD.

Responsável pelo Registro: Encarregado de Dados Pessoais (DPO). Contudo, as demais Unidades e Departamentos, quando for o caso, deverão fornecer, de forma tempestiva, todas as informações e evidências necessárias para subsidiar a análise e o registro do incidente, e **conferir prioridade ao atendimento** das solicitações do DPO envolvendo o incidente.

8.2 Conteúdo Mínimo do Registro

O processo no SGP-e (assunto 018) deve conter, obrigatoriamente:

- a) A data e hora do conhecimento do incidente;
- b) Descrição detalhada das circunstâncias (o que e como ocorreu);
- c) Natureza, categoria e quantidade de dados e titulares afetados;
- d) Avaliação de risco e possíveis danos aos titulares;
- e) Medidas de correção e mitigação já adotadas;
- f) Justificativa documentada em caso de decisão pela não comunicação à ANPD ou aos titulares.

8.3 Fluxo de tramitação

Após a abertura, o processo tramitará de forma dinâmica para coletar subsídios técnicos e jurídicos. O DPO coordenará o fluxo, podendo solicitar manifestações de qualquer unidade da Epagri, sendo as principais:

- a) Unidade de Origem: responsável por prestar esclarecimentos detalhados sobre a dinâmica do evento e auxiliar na identificação dos danos;
- b) DEGTI: atuará com pareceres sobre medidas técnicas adotadas antes do incidente, contenção, erradicação técnica, além de quantificar e qualificar os dados e sistemas envolvidos no incidente;
- c) DPO: responsável pela análise final de conformidade, registro das ações de mitigação e decisão sobre notificações externas (ANPD e titulares);
- d) Setores de Apoio (Equipe Específica para Tratamento de Incidentes de Maior Complexidade, DJUR, DEGP, DEMC, entre outros): poderão ser acionados para opinar sobre questões jurídicas, falhas humanas, medidas disciplinares ou estratégias de comunicação, conforme a necessidade e a critério do DPO.

9 CONTENÇÃO E ERRADICAÇÃO DO INCIDENTE DE SEGURANÇA

Esta fase visa identificar a extensão do dano e estancar a violação de dados de forma imediata, abrangendo tanto falhas tecnológicas quanto eventos físicos ou administrativos.

9.1 Avaliação Técnica e Funcional

O DEGTI (no caso de incidentes digitais) ou o Gestor da Unidade (no caso de incidentes não digitais) deve diagnosticar a causa-raiz e o método da violação para impedir a sua progressão. Para isso, deve-se identificar se o evento se enquadra em uma das categorias de possíveis incidentes da Epagri:

Incidentes Digitais:

- Sequestro de dados (*ransomware*) sem transferência de informações;
- Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações;
- Vírus de Computador/*Malware*;
- Exploração de vulnerabilidade ou falha em sistemas de informação (*software*);
- Acesso não autorizado a sistemas ou a dados, violando o seu sigilo;
- Roubo ou violação de credenciais (ex: engenharia social, força bruta, *phishing*);
- Negação de Serviço (DoS) ou indisponibilidade de acesso aos dados por período significativo;
- Alteração, exclusão ou destruição de dados de maneira não autorizada ou acidental;
- Divulgação, publicação ou envio indevido/acidental de dados pessoais a destinatário incorreto por meios digitais;
- Outro tipo de incidente cibernético.

Incidentes em meios físicos e administrativos (não cibernéticos):

- Perda, furto ou roubo de documentos físicos ou dispositivos eletrônicos corporativos;
- Descarte incorreto de documentos físicos ou mídias de armazenamento;
- Divulgação ou acesso não autorizado a informações físicas (ex: documentos sobre a mesa);
- Falha grave em equipamento (*hardware*) que afete a disponibilidade da informação;
- Outro tipo de incidente físico ou não cibernético.

9.2 Medidas de Contenção e Erradicação (Meios Digitais)

O objetivo é isolar a ameaça com apoio do DEGTI para limitar o impacto e preservar a integridade dos ativos:

- a) Isolamento: bloquear contas suspeitas ou isolar sistemas e funcionalidades comprometidas para evitar danos adicionais;
- b) Preservação de Evidências e Cadeia de Custódia: evitar a destruição de logs e provas digitais essenciais para a investigação forense e regulatória. A coleta de evidências deve documentar rigorosamente a cadeia de custódia, registrando: a identificação do ativo (IP, MAC, localização), o nome e a matrícula do usuário que manuseou a evidência, a data e a hora exata de cada manipulação, e o local seguro onde a evidência foi armazenada;
- c) Intervenção Direta: realizar o desligamento de sistemas inteiros ou funcionalidades específicas, caso a gravidade do ataque exija interrupção imediata.

9.3 Medidas de Contenção e Erradicação (Meios Não Digitais/Físicos)

Para incidentes originados por atividade humana ou falhas físicas, as ações são de natureza administrativa e operacional:

- a) Avaliação Setorial: realizar análise detalhada com o Gestor do setor responsável e apoio do DEGOP (para terceirizados) ou DEGP (para funcionários);
- b) Interrupção do Dano: recolher documentos expostos, restringir acessos físicos ou aplicar medidas disciplinares imediatas conforme a legislação aplicável;

- c) Formalização: documentar todas as interações, autorizações e medidas disciplinares para garantir que a contenção esteja alinhada às normas de proteção de dados.

10 RECUPERAÇÃO

O restabelecimento dos ambientes deve seguir os padrões técnicos de segurança estabelecidos na Política de Segurança da Informação, priorizando a correção da vulnerabilidade explorada.

São exemplos de medidas para recuperar os sistemas e mitigar riscos:

- Corrigir vulnerabilidades físicas e digitais que causaram o incidente;
- Tratamento do incidente, por exemplo, restauração de *backup* e restauração de sistemas; atualização de antivírus;
- Atualização da gestão de riscos, inclusive relacionados à proteção de dados pessoais.

Se necessário, revisar as medidas de segurança aplicáveis:

- a) Política de Privacidade e Proteção de Dados;
- b) Política de Segurança da Informação (POSIN);
- c) Plano de resposta a incidentes de segurança;
- d) Manutenção e atualização periódica do Inventário de Dados Pessoais (IDP) da Epagri;
- e) Criptografia;
- f) Anonimização;
- g) Antivírus;
- h) Registros de acessos (logs);
- i) Testes de invasão;
- j) Processos de gestão de riscos;
- k) Controle de acesso lógico;
- l) Cópias de segurança (backups);
- m) Firewall;
- n) Monitoramento de uso de rede e sistemas;
- o) Registro de incidentes;
- p) Segregação de rede;

- q) Gestão de ativos;
- r) Atualização de sistemas;
- s) Múltiplos fatores de autenticação;
- t) Aplicação rigorosa do Princípio do Privilégio Mínimo na concessão de acessos lógicos;
- u) Implementação de Sistemas de Prevenção e Detecção de Intrusão (IDS/IPS) e ferramentas de verificação de integridade de arquivos;
- v) Sincronização contínua de relógios de hosts via Network Time Protocol (NTP);
- w) Controle de acesso físico;
- x) Substituição de lacres, chaves ou trancas em arquivos físicos;
- y) Realização periódica de exercícios e simulações práticas de resposta a incidentes para capacitação da equipe técnica e administrativa;
- z) Outras.

11 COMUNICAÇÕES À ANPD E AO TITULAR DE DADOS PESSOAIS

Figura 4 – Comunicação à ANPD¹



Não é todo incidente de segurança que exige comunicação à ANPD. A decisão pela comunicação será fundamentada na Matriz de Impacto (Quadro 3) deste Plano e em conformidade com o art. 5º da Resolução CD/ANPD nº 15/2024 se envolver alguns dos seguintes dados pessoais:

- Dados pessoais sensíveis;
- Dados de crianças, de adolescentes ou de idosos;
- Dados financeiros;
- Dados de autenticação em sistemas;
- Por sigilo legal, judicial ou profissional; ou
- Dados em larga escala.

¹Fonte: ANPD (2024).

11.1 Prazos e Responsabilidades

O **prazo de comunicação é de até 3 (três) dias úteis** a partir do conhecimento do incidente pela Epagri. Caso a comunicação completa não seja possível nesse prazo, deverá ser realizada uma comunicação preliminar, devendo a Epagri fornecer informações complementares em até 20 dias úteis.

O responsável pela comunicação é o Encarregado de Dados.

A ANPD orienta cautela e precaução: em caso de dúvidas, a Epagri deve comunicar o incidente. Eventual e comprovada subavaliação dos riscos e danos por parte dos controladores de dados pode ser considerada descumprimento à legislação de proteção de dados pessoais.

11.2 Comunicações do Incidente ao Titular de Dados

No caso de incidente com vazamento de dados pessoais, o DPO, com o apoio multidisciplinar, deve coordenar as comunicações ao titular.

Deverá ser em linguagem **clara, simples, de forma direta e individualizada**, através de:

- Preferencialmente, comunicado individual por escrito (mensagem eletrônica, carta, e-mail, etc.);
- Anúncio público no *site*, mídias sociais ou aplicativos da Epagri;
- Ampla divulgação em meios de comunicação.

O comunicado ao titular de dados deve conter, ao menos:

- A descrição da natureza e da categoria de dados pessoais afetados;
- As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- Os motivos da demora, no caso de a comunicação não ter sido feita no prazo de três dias úteis;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- A data do conhecimento do incidente de segurança; e
- O contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

11.3 Relatório do Incidente à ANPD

A comunicação deve ser formalizada pelo DPO através do sistema eletrônico da ANPD e registrada internamente no SGP-e (Assunto 011). O **Relatório do Incidente**, com cópias de documentos físicos ou digitais, deve conter os seguintes elementos:

- a) A descrição da natureza e da categoria de dados pessoais afetados;
- b) O número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- c) As medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais e adotadas antes e após o incidente, observados os segredos comercial e industrial;
- d) Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares, sendo assim classificados: a) podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade; b) podem sofrer danos, superáveis com certa dificuldade; c) podem sofrer danos importantes, superáveis com muita dificuldade; d) podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou têm potencial para ocasionar dano significativo ou irreversível;
- e) Os motivos da demora, no caso de a comunicação não ter sido realizada no prazo de **3 (três) dias úteis**;
- f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- g) A data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pela Epagri;
- h) Os dados do encarregado ou de quem represente a Epagri;
- i) A identificação da Epagri;
- j) A identificação do operador, quando aplicável;
- k) A descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- l) O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

11.4 Padronização de resposta

Conforme as orientações da ANPD, a Epagri deve implementar procedimentos padronizados para comunicação de incidentes, assegurando clareza, tempestividade e a utilização de linguagem acessível, especialmente no contato com os titulares de dados.

Para garantir a agilidade operacional e facilitar a revisão, os modelos padronizados podem ser acessados na [Cadeia de Valor](#).

12 ADEQUAÇÃO E MELHORIA CONTÍNUA

A fase de melhoria contínua tem como objetivo aprimorar os processos de resposta a incidentes, reduzir recorrências e fortalecer os controles de segurança da informação e proteção de dados pessoais.

12.1 Diretrizes gerais

- **Documentação e Ações Corretivas:** as medidas corretivas deverão incluir a documentação detalhada das vulnerabilidades identificadas e das ações adotadas para sua mitigação.
- **Registro e Conformidade (ANPD):** em relação à proteção de dados pessoais, deverá ser mantido registro completo das ações de contenção, eliminação e mitigação, conforme a Resolução [CD/ANPD nº 15/2024](#). Seguindo o [Plano de Classificação e Tabela de Temporalidade de Documentos da Administração Pública do Estado de Santa Catarina \(Atividades-Meio\)](#), a guarda será permanente. Nos dois casos de registro (Comunicação de Incidentes e Processo de Incidentes - assuntos 011 e 018, respectivamente), as fases corrente e intermediária serão de **10 anos** cada.
- **Base de Conhecimento:** as lições aprendidas deverão ser formalmente registradas em uma Base de Conhecimento de Incidentes, servindo como um repositório interno com o histórico e as táticas de eventos passados para agilizar tratativas futuras.
- **Atualização da Gestão de Riscos:** as informações consolidadas no relatório final do incidente deverão ser incorporadas aos processos de gestão de riscos e de segurança da informação.
- Essas informações consolidadas serão obrigatoriamente utilizadas como subsídio para revisar e atualizar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) da Epagri.

12.2 Metodologia de Melhoria Contínua

Figura 5 – Ciclo PDCA²



Deverá ser aplicado o ciclo PDCA (*Plan, Do, Check, Act* – Planejar, Executar, Checar e Agir), utilizando os resultados das análises de incidentes para retroalimentar a gestão de riscos e os controles de segurança.

12.3 Monitoramento e indicadores

Poderão ser utilizados indicadores para avaliação da eficácia do processo de resposta a incidentes, tais como:

- a) Tempo de resposta;
- b) Tempo de resolução;
- c) Reincidência de incidentes.

12.4 Reuniões de lições aprendidas

Após a ocorrência de incidentes relevantes, deverão ser realizadas reuniões para análise e identificação de melhorias no processo de resposta a incidentes.

Sugere-se a análise dos seguintes aspectos:

- Onde, quando, como e o que ocorreu;
- Eficácia das ações adotadas;
- Adequação dos procedimentos existentes;
- Necessidade de criação ou revisão de procedimentos;
- Informações necessárias para resposta ao incidente;
- Eventuais falhas que tenham prejudicado a recuperação;
- Oportunidades de melhoria no tratamento de incidentes;
- Aprimoramento do compartilhamento de informações;
- Ações corretivas para evitar recorrência;
- Indicadores e sinais de alerta para detecção futura;
- Recursos adicionais necessários para prevenção e resposta.

²Fonte: Vecteezy.com (2026).

13 RELATÓRIO DE TRATAMENTO DE INCIDENTE

O Relatório de Tratamento de Incidente deve conter 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. Ele poderá ser solicitado pela ANPD a qualquer tempo, com o propósito de:

- Avaliar as ações tomadas durante um incidente em que dados pessoais tenham sido expostos ou comprometidos;
- Publicar e atualizar normas referentes à proteção de dados;
- Cumprir o princípio da responsabilização e da prestação de contas (art. 6º, inciso X da LGPD);
- Utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

Para a Epagri o Relatório de Tratamento é importante, pois conterá as devidas considerações para a promoção da melhoria contínua dos processos de tratamento de incidentes e pode incluir resumidamente: as informações obtidas, a linha de tempo, os atores envolvidos, as evidências, as conclusões, as decisões, as autorizações e as ações tomadas; podendo, inclusive, ser acrescentada às decisões de sensibilização dos funcionários a Revisão do Plano.

Essa documentação deverá ser registrada no mesmo SGP-e do Incidente de Segurança (Assunto 018), garantindo que o registro atenda aos requisitos da Resolução CD/ANPD nº 15/2024 para auditoria e comprovação de conformidade.

14 ENCERRAMENTO FORMAL DO INCIDENTE

O incidente de dado pessoal será considerado encerrado quando:

- a) As ações de contenção e recuperação estiverem concluídas;
- b) O registro estiver completo;
- c) As comunicações obrigatórias tiverem sido realizadas;
- d) O relatório final tiver sido elaborado.

15 SENSIBILIZAÇÃO DOS FUNCIONÁRIOS E REVISÃO DO PLANO

Em caso de **incidentes de nível de risco Alto**, o DPO e o DEGTI deverão agendar e conduzir uma reunião, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos – inclusive deste Plano de Resposta a Incidentes.

As reuniões devem ser formalizadas em atas documentadas, com atribuição de prazos para implementação das melhorias identificadas e recomendações do DPO e do DEGTI, quando aplicáveis.

As melhorias sugeridas na reunião, após o devido consenso, deverão ser encaminhadas à Diretoria Executiva para definição quanto à sua adoção.

16 FLUXO – CADEIA DE VALOR

Os fluxogramas e documentos referentes ao Plano de Resposta a Incidentes de Segurança da Informação podem ser acessados na [Cadeia de Valor da Epagri](#).

17 GLOSSÁRIO

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. É irreversível e perde a qualidade de dado pessoal para fins de LGPD.

Agência Nacional de Proteção de Dados (ANPD): autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018 (LGPD) em todo o território nacional.

Cadeia de Custódia: processo rigoroso e documentado que registra cronologicamente a coleta, posse, controle, transferência e análise de evidências físicas ou digitais. Seu objetivo é garantir a integridade, rastreabilidade e validade legal das provas para fins de auditoria, processos administrativos ou judiciais.

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.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado de Autenticação em Sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou confirmar a identificação de um usuário, como contas de login, tokens e senhas.

Dado Pessoal Afetado: é o dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança.

Dado Pessoal: toda e qualquer 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.

Dados Protegidos por Sigilo (Legal, Judicial ou Profissional): dado pessoal cujo sigilo decorra de norma jurídica, decisão judicial ou do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem.

Encarregado de dados: pessoa indicada pelo controlador (Epagri) e operador para atuar como canal de comunicação entre o controlador (Epagri), os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

Incidente com Dados em Larga Escala: incidente que abrange 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.

Incidente de Segurança da Informação com Dados Pessoais: é um evento adverso confirmado que compromete as propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda, indisponibilidade ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados. A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança.

Incidente de Segurança da Informação – Digital: incidente que envolve sistemas de informação, redes, equipamentos ou ativos tecnológicos, cuja análise e tratamento técnico são de responsabilidade do DEGTI.

Incidente de Segurança da Informação – Não Digital: incidente que não envolve sistemas de informação ou ativos tecnológicos, caracterizado por eventos físicos, administrativos ou comportamentais que possam comprometer a confidencialidade, integridade ou disponibilidade das informações, tais como acesso indevido a documentos físicos, extravio de documentos, divulgação indevida de informações em meio não eletrônico ou falhas em controles administrativos.

Inventário de Dados Pessoais (IDP): Artefato primordial que documenta e mapeia todos os processos de tratamento de dados pessoais realizados pela instituição, identificando a fonte, o fluxo, as bases legais e as medidas de segurança aplicadas.

Medidas de segurança: são medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Natureza dos dados pessoais: de acordo com a ANPD, classificação de dados pessoais em gerais ou sensíveis.

Network Time Protocol (NTP): protocolo de rede utilizado para sincronizar de forma precisa os relógios dos computadores e servidores. É uma configuração essencial de segurança para facilitar a correta correlação temporal de eventos e análise de logs durante a investigação de um incidente.

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

Princípio do Privilégio Mínimo: prática de governança e segurança da informação que determina que a um usuário, sistema ou processo devem ser concedidos apenas os níveis de acesso e as permissões estritamente necessárias para a execução de suas funções previamente autorizadas.

Pseudonimização: é o tratamento no qual um dado perde a capacidade de associação a um indivíduo, exceto pelo uso de informação adicional mantida separadamente pela Epagri em ambiente seguro. A reidentificação ainda é possível e por isso não perde a qualidade de dados pessoais para fins de LGPD.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que têm o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como as medidas, salvaguardas e os mecanismos adotados para a mitigação desses riscos.

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.

Risco ou dano relevante aos titulares: 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.

Sistemas de Prevenção e Detecção de Intrusão (IDS/IPS): ferramentas de segurança de rede projetadas para monitorar o tráfego em busca de atividades maliciosas ou violações de políticas. O Sistema de Detecção (IDS) emite alertas sobre anomalias, enquanto o Sistema de Prevenção (IPS) atua bloqueando ou impedindo a ameaça em tempo real.

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

Tratamento de Dados: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuário: empregado público, estagiário, bolsista, aprendiz, empregado ou servidor público à disposição de outras instituições, empregado ou servidor público cedido por outras instituições, prestadores de serviço voluntário, terceirizados, instrutores, alunos e demais colaboradores que estão autorizados a utilizar a rede, os equipamentos de informática e os sistemas de informação das Unidades da Epagri.

18 REFERÊNCIAS

BRASIL. Agência Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. **Diário Oficial da União**: seção 1, Brasília, DF, 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 26 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. **Comunicação de Incidentes de Segurança, 2026**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 18 fev. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 fev. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia de Resposta a Incidentes de Segurança**: Programa de Privacidade e Segurança da Informação (PPSI). Versão 3.3. Brasília: SGD/MGI, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf. Acesso em 22 jun. 2026.

SANTA CATARINA. Secretaria de Estado da Administração. **Instrução Normativa SEA nº 003, de 11 de março de 2019**. Estabelece os procedimentos para a gestão de documentos e processos eletrônicos no âmbito do Poder Executivo Estadual. **Diário Oficial [do] Estado de Santa Catarina**. Florianópolis, ano LXXXV, n. 20971, p. 1-6, 2019. Disponível em: <https://portal.doe.sea.sc.gov.br/v2.44.07/#/portal/edicao/buscar-edicao>. Acesso em 10 abr. 2026.



www.epagri.sc.gov.br



www.youtube.com/epagritv



www.facebook.com/epagri



www.instagram.com/epagri



linkedin.com/company/epagri



<http://publicacoes.epagri.sc.gov.br>



www.x.com/EpagriOficial