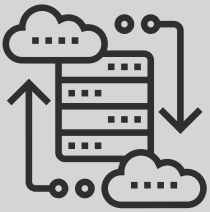

Guilherme Rafael de Souza Araujo

GUERRA DOS DADOS

Cibergovernança e Soberania Financeira

2027

EDITORA JusPODIVM

www.editorajuspodivm.com.br

APÊNDICE I – MODELOS DE DEFESA E COMUNICAÇÃO À ANPD

PARTE 1/2 – COMUNICAÇÃO DE INCIDENTE + CASO FICTÍCIO

1. OBJETIVO E USO PRÁTICO

Este Apêndice I reúne **modelos operacionais** para atuação perante a Autoridade Nacional de Proteção de Dados (ANPD), com foco em:

- comunicação de **incidentes de segurança**;
- respostas a **diligências**;
- preparação de **defesas administrativas**;
- apoio à **governança pós-incidente**,

sempre dentro do contexto da **Guerra dos Dados** e da **soberania informacional**.

Nesta **Parte 1**, você encontra:

- diretrizes gerais de uso dos modelos;
- **Modelo 1 – Comunicação de incidente de segurança à ANPD** (art. 48 da LGPD);
- **Caso fictício preenchido** (fintech / sistema financeiro) para ilustrar o uso prático do modelo.

A **Parte 2** (a seguir, neste mesmo Apêndice I) traz:

- **Modelo 2 – Ofício de resposta e complementação de informações à ANPD**;
- **Modelo 3 – Defesa administrativa em processo sancionador**;
- **Modelo 4 – Estrutura simplificada de RIPD pós-incidente**;
- **Checklist pós-incidente**, para uso interno.

Tudo pensado para ser usado, em conjunto, por **compliance**, **jurídico**, **DPO**, **PLD/FT**, **tecnologia** e **governança**.

2. DIRETRIZES GERAIS DE UTILIZAÇÃO

Antes de entrar no Modelo 1, algumas **regras de ouro** para evitar erro estratégico:

(a) Nunca copiar "no piloto automático"

- Os modelos são **estruturais**, não "peças prontas para protocolo".
- Devem sempre ser adaptados:
  - ao **porte da organização**;
  - ao **setor** (público/privado, financeiro, saúde, varejo etc.);
  - ao **tipo de incidente** (ransomware, erro humano, falha de sistema, terceiro etc.);
  - ao **nível de maturidade** em privacidade e segurança.

(b) Incidente de segurança ≠ fracasso total de governança

A narrativa nunca deve ser de "terra arrasada". A linha de defesa central é mostrar que:

- já existiam **controles minimamente razoáveis** antes do incidente;
- houve **reação tempestiva**, com resposta estruturada;
- foram adotadas **medidas corretivas estruturais**, e não apenas "remendos" pontuais.

(c) Consistência entre ANPD, BACEN, COAF, CVM

Se o incidente envolver:

- **dados financeiros**;
- **Open Finance**;
- **meios de pagamento**;
- **mercado de capitais**,

então é essencial garantir que:

- a narrativa de fatos enviada à ANPD **não contradiga** as comunicações a BACEN, COAF ou CVM;
- o **fato seja um só**, com ajustes apenas de **enfoque regulatório** (privacidade, PLD/FT, prudencial, mercado de capitais).

(d) Não prometa o que não consegue entregar

- Se a **causa raiz** ainda é desconhecida, diga que **está em apuração** e assuma compromisso explícito de **complementar**.

- Se a **estimativa de titulares afetados** ainda pode mudar, deixe claro que: "Trata-se de estimativa preliminar, sujeita a ajuste à medida que a investigação avança."

(e) Documente tudo internamente

Por trás de uma comunicação de 2–3 páginas idealmente existem:

- **relatório técnico** (linha do tempo, causa provável, impactos);
- **ata ou registro de decisão** (comitê, diretoria, DPO);
- **trilha de auditoria** de logs, evidências e medidas adotadas.

Isso:

- protege a instituição em eventual fiscalização;
- serve de base para **defesa futura** em processo sancionador ou judicial.

3. MODELO 1 – COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA À ANPD

(Art. 48 da LGPD – estrutura comentada + modelo "seco")

3.1. Estrutura comentada (para o advogado/DPO entender a lógica)

Bloco A – Identificação básica

- Quem está comunicando (controlador);
- Quem assina (representante legal e/ou DPO);
- CNPJ, endereço, contatos;
- Canal de contato do DPO.

Bloco B – O incidente em si

- Quando foi detectado;
- Onde ocorreu (sistema, ambiente, fornecedor, data center, nuvem etc.);
- Qual o tipo de incidente:
  - acesso não autorizado;
  - vazamento;
  - indisponibilidade;
  - perda ou destruição de dados;
  - outro evento de segurança relevante.

Bloco C – Dados e titulares atingidos

- Tipos de dados:
  - cadastrais;
  - financeiros;
  - credenciais;
  - sensíveis;
  - logs de acesso, localização etc.;
- Quantidade de titulares afetados (ainda que **estimativa**);
- Presença ou não de **grupos vulneráveis** (crianças, adolescentes, idosos, pessoas em situação de vulnerabilidade socioeconômica).

Bloco D – Causa provável e riscos

- O que se sabe até agora sobre a **causa provável** (mesmo que em caráter preliminar);
- Quais **riscos concretos** os titulares correm, como:
- fraude financeira;
- phishing e golpes;
- discriminação;
- dano reputacional;
- uso indevido em outras bases ilícitas.

Bloco E – Medidas adotadas

- **Contenção** (parar o "sangramento"): bloqueios, isolamento de sistemas, revogação de credenciais;
- **Mitigação** (reduzir os danos): monitoramento reforçado, ajustes de acesso, avisos internos;
- **Medidas estruturais**: revisão de políticas, treinamentos, revisão de contratos com operadores, melhoria tecnológica.

Bloco F – Comunicação a titulares

- Se já comunicou: como, quando e por quais canais;
- Se ainda vai comunicar: em que prazo e por qual meio;
- Se entende, de forma fundamentada, que **não precisa** comunicar: explicitar claramente o **fundamento jurídico e técnico** (ex.: dados cifrados, baixo risco, impossibilidade prática de uso indevido etc.).

Bloco G – Situação atual e compromisso de complementar

- Se a investigação está em andamento ou em fase de conclusão;
- O que já se sabe e o que ainda está em apuração;
- O compromisso formal de **enviar informações adicionais** à ANPD assim que surgirem elementos relevantes.

3.2. Modelo 1 – Versão "seca", pronta para adaptação

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS (Art. 48 da Lei nº 13.709/2018 – LGPD)

À
Autoridade Nacional de Proteção de Dados – ANPD

Assunto: Comunicação de incidente de segurança envolvendo dados pessoais – art. 48 da Lei nº 13.709/2018 (LGPD)

[NOME COMPLETO DO CONTROLADOR], pessoa jurídica de direito [público/privado], inscrita no CNPJ sob o nº [•], com sede na [endereço completo], neste ato representada por seu [representante legal] e por seu Encarregado pelo Tratamento de Dados Pessoais (DPO), [nome do representante / DPO], vem, respeitosamente, à presença dessa Autoridade Nacional de Proteção de Dados, com fundamento no art. 48 da Lei nº 13.709/2018 (LGPD), **comunicar a ocorrência de incidente de segurança envolvendo dados pessoais**, nos termos a seguir expostos.

1. Identificação do incidente de segurança

1.1. Data e hora da detecção

O incidente de segurança foi detectado em [data], às [hora], no contexto de [breve contexto: monitoramento de logs, alerta de sistema de segurança, reporte de terceiro, teste interno etc.].

1.2. Ambiente e sistemas afetados

O evento ocorreu no ambiente **[interno / terceirizado / nuvem / híbrido]**, afetando, até o momento, os seguintes sistemas e/ou bases de dados:

- **[nome do sistema / base 1]** – [descrição objetiva da função];
- **[nome do sistema / base 2]** – [descrição objetiva da função].

1.3. Natureza do incidente

Trata-se de incidente de segurança caracterizado por [**acesso não autorizado/vazamento/exposição indevida/perda/destruição/indisponibilidade/outro**], conforme evidências técnicas preliminares.

2. Categoria e volume de dados pessoais envolvidos

2.1. Categorias de dados pessoais

Com base na análise realizada até o presente momento, o incidente envolveu:

a) dados **pessoais comuns**, relacionados a [clientes/usuários/empregados/fornecedores/outros], tais como [ex.: nome, CPF, e-mail, dados de contato, informações de transações]; e/ou

b) dados **pessoais sensíveis**, consistentes em [ex.: dados de saúde, dados biométricos, convicções religiosas, dados de crianças/adolescentes], se aplicável.

Quando ainda houver incerteza, pode ser consignado:

> "Até o momento, não foi possível confirmar, com segurança, o envolvimento de dados pessoais sensíveis, permanecendo a investigação em curso."

2.2. Quantidade estimada de titulares afetados

A quantidade **estimada** de titulares potencialmente afetados é de aproximadamente [**número ou faixa estimada**], com base em [**critério utilizado: volume de registros na base, janela temporal de processamento, logs de acesso etc.**].

2.3. Grupos vulneráveis

Até o momento, verificou-se a possível afetação de dados de [**crianças/adolescentes/idosos/pessoas em situação de vulnerabilidade socioeconômica/não identificados**], em razão de [**breve explicação**].

Caso não haja evidência nesse sentido, pode-se registrar:

> "Até o momento, não há evidência de envolvimento de dados de crianças, adolescentes ou outros grupos vulneráveis."

3. Descrição do incidente e causas prováveis

3.1. Descrição factual

Em [**data do fato principal**], foi identificado que [**descrever, de forma cronológica e objetiva, o que ocorreu: ex.: um terceiro obteve acesso**

indevido a credenciais, houve extração não autorizada de dados, envio equivocado de arquivos, falha em atualização de sistema, ataque de ransomware etc.].

3.2. Causa provável

Com base na investigação preliminar conduzida por [**área interna / equipe multidisciplinar / empresa especializada**], a causa provável do incidente está relacionada a:

- [**falha técnica**] em [infraestrutura / aplicação / configuração de segurança]; e/ou
- [**falha humana**], consistente em [erro operacional, descumprimento de procedimento, falha de validação]; e/ou
- [**ação maliciosa de terceiro**], caracterizada por [phishing, malware, ransomware, exploração de vulnerabilidade, engenharia social etc.].

Se ainda não houver definição segura, pode-se consignar:

> "As investigações encontram-se em curso, não sendo possível, neste momento, apontar com segurança a causa raiz do incidente, o que será oportunamente complementado a essa Autoridade."

4. Riscos aos direitos e liberdades dos titulares

A partir da análise de risco realizada em [**data**], foram identificados, em tese, os seguintes riscos:

a) risco de **utilização indevida dos dados** para fins de [fraude financeira, abertura indevida de contas, phishing, golpes, discriminação etc.];
b) risco de **exposição indevida de informações** de natureza [financeira, trabalhista, de saúde, educacional, outra];
c) possibilidade de [**acesso não autorizado por terceiros / cruzamento com outras bases / reidentificação de titulares**], quando aplicável.

Quando o risco for considerado **baixo ou moderado**, pode-se acrescentar:

> "Considerando as características técnicas do incidente, a natureza dos dados pessoais envolvidos e as medidas de contenção adotadas, entende-se que o risco aos direitos e liberdades dos titulares se apresenta, neste momento, como [**baixo/moderado**], sem prejuízo do monitoramento contínuo e da comunicação transparente com os afetados, quando exigível."

5. Medidas técnicas e administrativas adotadas

5.1. Medidas de contenção imediata

Foram adotadas, entre outras, as seguintes medidas:

- bloqueio de [**contas/credenciais/perfis**] associados ao incidente;
- isolamento de [**servidores/estações/ambientes em nuvem**] potencialmente afetados;
- suspensão temporária de [**serviços/funcionalidades/integrações**] para interromper o vetor de ataque.

5.2. Medidas de mitigação

Em sequência, foram implementadas:

- revisão de perfis de acesso e reforço da autenticação dos usuários;
- monitoramento intensificado de logs e alertas de segurança;
- comunicação interna às áreas impactadas, com orientações específicas;
- comunicação a operadores e terceiros envolvidos, solicitando cooperação na mitigação.

5.3. Medidas estruturais

Como desdobramento do incidente, foram iniciadas:

- revisão e atualização das **políticas de segurança da informação e privacidade**;
- reforço de **treinamentos e campanhas internas**;
- reavaliação de **contratos com terceiros** que tratam dados para a organização.

6. Comunicação aos titulares (quando aplicável)

Informa-se que:

- os titulares foram comunicados em [**data**], por meio de [**e-mail, SMS, área logada, carta, comunicado público, combinação de meios**]; ou
- a comunicação aos titulares está em fase de planejamento, com previsão de conclusão em [**prazo estimado**]; ou
- entende-se, de forma fundamentada, que **não é necessária comunicação individualizada**, pelos seguintes motivos: [**fundamentação jurídica e técnica – risco baixo, dados cifrados, ausência de possibilidade de uso indevido etc.**].

7. Situação atual da investigação

A investigação interna encontra-se em [**andamento / fase de conclusão**], sob responsabilidade de [**área / comitê / empresa especializada**].

Até o momento, concluiu-se que:

- [**síntese das principais conclusões técnicas já apuradas**];
- permanecem pendentes de esclarecimento os pontos [**listar, se houver**].

O Controlador **compromete-se a complementar** as informações ora prestadas tão logo sejam obtidos novos elementos relevantes.

8. Dados de contato

Para esclarecimentos adicionais, a ANPD poderá contatar:

- **Nome do Encarregado (DPO):** [nome completo]
- **Cargo/Função:** [•]
- **E-mail institucional:** [•]
- **Telefone:** [•]
- **Endereço para correspondência:** [•]

9. Declaração final

À vista do exposto, [**NOME DO CONTROLADOR**] cumpre o dever de comunicar incidente de segurança envolvendo dados pessoais, nos termos do art. 48 da LGPD, colocando-se à disposição dessa Autoridade para:

- prestar esclarecimentos adicionais;
- acompanhar a apuração dos fatos;
- implementar as medidas de governança necessárias à prevenção de novos incidentes.

[Município], [data].

[Nome do representante legal]
[Cargo]
[Nome do Controlador]

[Nome do Encarregado (DPO), se assinar conjuntamente]
[Cargo/Função]
[Nome do Controlador]

4. CASO FICTÍCIO – INCIDENTE EM FINTECH (EXEMPLO PREENCHIDO)

Atenção: este caso é totalmente fictício. Serve apenas para demonstrar como o Modelo 1 pode ser aplicado na prática, em contexto financeiro / Open Finance.

4.1. Cenário resumido

- **Controlador:** Banco Digital Atlas S.A., instituição de pagamento voltada para conta digital e cartão pré-pago.
- **Incidente:** acesso indevido a base de **logs de API de Open Finance**, com exposição de dados cadastrais e parte do histórico de transações.
- **Vetor:** credenciais de API comprometidas por **phishing direcionado** a desenvolvedor de empresa terceirizada de tecnologia.
- **Dados sensíveis:** não (sem dados de saúde, biometria, crenças etc.), mas com **alto risco financeiro** pela possibilidade de fraude.

4.2. Principais trechos do modelo preenchidos

4.2.1. Identificação do incidente

O incidente de segurança foi detectado em **02/08/2025**, às **03h17**, a partir de alerta automatizado do sistema de monitoramento de APIs, que identificou **padrão atípico de requisições**, em volume concentrado e fora do horário usual, direcionadas ao ambiente de Open Finance do Banco Digital Atlas S.A.

O evento afetou o **ambiente em nuvem** utilizado para processamento de requisições de API de Open Finance, especificamente a **base de logs de transações e consultas** destinada à conciliação e auditoria.

Trata-se de incidente caracterizado por **acesso não autorizado e extração indevida de dados** contidos em logs de API, segundo análise preliminar da equipe de segurança da informação.

4.2.2. Dados e titulares

A análise inicial indica o envolvimento de **dados pessoais comuns** de clientes e ex-clientes do Banco Digital Atlas S.A., tais como:

- nome;
- CPF;
- e-mail;
- telefone;
- identificadores de contas;
- valores e datas de determinadas transações financeiras.

Não foram identificados **dados pessoais sensíveis** nos registros acessados.

Estima-se que aproximadamente **18.500 titulares** possam ter sido potencialmente afetados, com base em **amostragem dos logs extraídos** e cruzamento com a base de clientes ativos e inativos.

Até o momento, **não há evidência de envolvimento de dados de crianças ou adolescentes**.

4.2.3. Causa provável

A investigação preliminar aponta como causa provável do incidente o **comprometimento de credenciais de acesso** de um desenvolvedor terceirizado, vinculado a fornecedor de tecnologia, em razão de ataque de **phishing direcionado**, no qual o agente malicioso obteve usuário e senha válidos para acesso a ambiente de desenvolvimento e, a partir daí, explorou **permissões indevidamente configuradas** no ambiente de produção.

4.4.4. Riscos identificados

Os principais riscos identificados são:

a) utilização **indevida dos dados** para fraudes financeiras, inclusive tentativa de engenharia social (phishing) junto aos titulares, a partir da correlação entre dados cadastrais e histórico de transações;
b) exposição **de informações financeiras sensíveis em sentido econômico**, como padrões de consumo, datas e valores de operações, com potencial de afetar a privacidade e a segurança econômica dos titulares;
c) possibilidade de **correlação com outras bases ilícitas de dados**, intensificando golpes financeiros e ataques direcionados.

4.4.5. Medidas adotadas

Imediatamente após a detecção, o Banco Digital Atlas S.A.:

- revogou as **credenciais comprometidas** e bloqueou o acesso do usuário terceirizado;
- isolou temporariamente o **ambiente de APIs de Open Finance** para análise de integridade;
- ajustou as **permissões entre ambientes de desenvolvimento e produção**, restringindo acessos e segmentando privilégios;
- elevou o nível de **monitoramento transacional** para os titulares potencialmente afetados, com foco em detecção de operações atípicas;

- iniciou processo de **revisão de contratos** com o fornecedor envolvido, reforçando obrigações de segurança, notificação tempestiva de incidentes e treinamento.

4.4.6. Comunicação a titulares

Em **05/08/2025**, o Banco Digital Atlas S.A. iniciou a **comunicação individualizada** aos titulares potencialmente afetados, por meio de:

- e-mail; e
- mensagens na área logada do aplicativo,

informando:

- a ocorrência do incidente;
- os tipos de dados envolvidos;
- **orientações de segurança** (não compartilhamento de senhas, atenção a mensagens suspeitas, canais oficiais de atendimento);
- **canais disponíveis** para esclarecimentos adicionais e exercício de direitos.

4.4.7. Situação atual

Na data da comunicação à ANPD:

- a investigação interna encontra-se **em curso**, com apoio de empresa de segurança da informação contratada especificamente para o caso;
- **não há evidência** de uso efetivo dos dados em fraudes consumadas diretamente relacionadas ao incidente;
- foram **reforçados controles de acesso e monitoramento**, com base em recomendações técnicas preliminares;
- está em elaboração **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** específico para a operação de Open Finance, a fim de reavaliar os riscos e adequar controles de forma estruturada.

PARTE 2/2 – RESPOSTA, DEFESA, RIPD E CHECKLIST

Nesta segunda parte do Apêndice I, você encontra:

- **Modelo 2 – Ofício de resposta/complementação à ANPD**;
- **Modelo 3 – Defesa administrativa em processo sancionador**;
- **Estrutura prática de RIPD pós-incidente**;

- **Checklist operacional pós-incidente** para uso interno;
- Comentários com **casos fictícios** para orientar a aplicação prática.

1. MODELO 2 – OFÍCIO DE RESPOSTA E COMPLEMENTAÇÃO DE INFORMAÇÕES À ANPD

Finalidade: responder a ofícios, pedidos de esclarecimentos ou diligências da ANPD, mantendo **coerência** com a comunicação inicial do incidente (Modelo 1) e demonstrando **boa-fé, transparência e governança**.

MODELO – OFÍCIO DE RESPOSTA / COMPLEMENTAÇÃO

Campos entre colchetes devem ser preenchidos conforme o caso concreto. Ajuste o tom conforme o grau de criticidade do processo.

À

Autoridade Nacional de Proteção de Dados – ANPD

Assunto: Resposta a pedido de informações / complementação de dados – Processo nº [•]

Referência: Ofício nº [•], de [data]

[NOME COMPLETO DO CONTROLADOR], pessoa jurídica de direito [público/privado], inscrita no CNPJ sob o nº [•], com sede na [endereço completo], neste ato representada por seu [representante legal] e por seu Encarregado pelo Tratamento de Dados Pessoais (DPO), [nome do DPO], vem, respeitosamente, à presença dessa Autoridade Nacional de Proteção de Dados, em atenção ao Ofício nº [•], referente ao Processo nº [•], apresentar as seguintes **informações e esclarecimentos complementares**.

1. Síntese do pedido formulado por essa Autoridade

Em **[data de recebimento]**, **[nome do controlador]** recebeu o Ofício nº [•], por meio do qual essa Autoridade solicitou, em síntese:

a) esclarecimentos adicionais sobre **[incidente de segurança / prática de tratamento / base legal / atendimento a direito de titular etc.]**;

b) encaminhamento de documentos comprobatórios relativos a **[listar: políticas, registros de logs, contratos com operadores, relatórios técnicos, comunicações a titulares etc.]**;

c) detalhamento das medidas técnicas e administrativas adotadas após o incidente relatado e do estágio da investigação interna.

Para fins de objetividade, esta resposta está organizada **item a item**, conforme a ordem estabelecida no Ofício nº [•].

2. Atualização do contexto fático

Desde a comunicação inicial apresentada em **[data]**, foram realizadas as seguintes ações internas:

a) constituição de **equipe multidisciplinar** (jurídico, privacidade/DPO, segurança da informação, TI, negócios, compliance) para apuração do incidente;
b) análise de **logs e trilhas de auditoria** referentes aos sistemas [X, Y, Z];
c) realização de **entrevistas com colaboradores** e, quando aplicável, solicitação formal de informações a operadores e terceiros envolvidos no tratamento.

Como resultado, foi possível **confirmar e/ou ajustar** as informações anteriormente comunicadas:

- **Situação inicialmente comunicada (resumo):** [Ex.: estimativa preliminar de 5.000 titulares; possível acesso indevido a dados cadastrais em ambiente de teste etc.]
- **Situação atual, após apuração complementar:** [Ex.: confirmação de 3.427 titulares afetados; delimitação do período de exposição entre 10/03/2025 e 14/03/2025; ausência de evidência de acesso a dados sensíveis; identificação de origem do evento em falha de configuração de ambiente em nuvem etc.]

Quando houver retificação relevante:

"Ressalte-se que, à luz dos novos elementos coletados, foi possível retificar a estimativa inicialmente informada quanto a [número de titulares / categorias de dados / duração do evento], mantendo-se o compromisso desta instituição com a exatidão e a transparência das informações prestadas a essa Autoridade."

3. Resposta aos itens específicos do Ofício nº [•]

Sugestão prática: copie cada item do Ofício e responda logo abaixo, de forma direta e objetiva.

Item 1 – [Transcrever ou resumir a pergunta da ANPD]

Resposta:

[Apresentar explicação clara, com datas, dados objetivos, sistemas envolvidos, fluxos de tratamento e, se pertinente, referência a documentos anexos.]

Item 2 – [Transcrever ou resumir]

Resposta:

[Explicar a base legal invocada, a lógica da escolha da base (art. 7º ou 11 da LGPD), a finalidade do tratamento, eventuais limitações, critérios de minimização de dados etc.]

Item 3 – [Transcrever ou resumir]

Resposta:

[Responder de forma pontual: se pediram fluxograma, descrevê-lo ou informar que segue anexo; se pediram cópia de políticas, indicar o documento e a data da aprovação; se pediram detalhamento de medidas de segurança, relacioná-las de forma organizada.]

(Repita essa estrutura para todos os itens do ofício.)

4. Medidas técnicas e administrativas adicionais adotadas

Em continuidade às medidas emergenciais já comunicadas, [**nome do controlador**] informa que:

4.1. Medidas técnicas

- **a)** revisão de perfis de acesso em sistemas críticos, reforçando o **princípio do menor privilégio**;
- **b)** implementação/fortalecimento de **autenticação multifator** para acessos administrativos e remotos;
- **c)** ampliação do escopo de **monitoramento de logs e alertas de segurança**, com regras específicas relacionadas ao tipo de incidente ocorrido;
- **d)** correção definitiva da vulnerabilidade identificada, com validação por meio de [**testes de segurança/varreduras de vulnerabilidade/avaliação independente**].

4.2. Medidas organizacionais e de governança

- **a)** atualização das **políticas de segurança da informação e de proteção de dados**, incorporando lições aprendidas com o incidente;

b) realização de **treinamentos complementares** para as áreas mais impactadas (ex.: atendimento, TI, operações);
c) revisão do **fluxo de comunicação de incidentes**, incluindo gatilhos objetivos para notificação à ANPD e aos titulares;
d) revisão de **contratos e cláusulas de proteção de dados com operadores**, prevendo obrigações reforçadas de notificação de incidentes e segurança.

4.3. Medidas em andamento

a) [Ex.: contratação de solução adicional de DLP, implementação de SOC terceirizado, revisão de arquitetura em nuvem etc.];
b) elaboração ou revisão de **Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)** das operações afetadas;
c) inclusão de **indicadores de segurança e privacidade** em painéis de governança reportados à alta administração.

5. Documentos anexos

Anexamos a este ofício, para fins de comprovação:

a) [Política de Segurança da Informação – versão atualizada em dd/mm/aaaa];
b) [Fluxograma ou diagrama da operação de tratamento relacionada ao incidente];
c) [Relatório técnico resumido da área de segurança da informação ou de consultoria especializada];
d) [Comunicado enviado aos titulares, se aplicável]; e) [Outros documentos relevantes].

Caso haja documentos sensíveis, pode-se registrar:

> "Determinados documentos de caráter técnico e sensível, por exigirem tratamento reservado, serão disponibilizados por meio de canal seguro a ser acordado com essa Autoridade, caso assim seja entendido por Vossas Senhorias como necessário."

6. Compromisso de cooperação e melhoria contínua

A [**nome do controlador**] reitera seu compromisso com:

a) a **cooperação integral** com essa Autoridade Nacional, fornecendo informações adicionais sempre que solicitado;