

# PERFUR DO BRASIL LTDA.

## PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

Procedimentos para prevenção, identificação, tratamento e comunicação de incidentes

Documento destinado à disponibilização no website da empresa

Versão 1.0 – 23 de setembro de 2026

### PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

A Perfur do Brasil Ltda., empresa do segmento de fabricação de brincos, com aproximadamente 34 colaboradores, adota este Plano de Resposta a Incidentes de Segurança da Informação Envolvendo Dados Pessoais (“Plano de Resposta” ou “PRI”) para estabelecer as providências aplicáveis quando houver identificação ou mera suspeita de incidente envolvendo dados pessoais tratados pela Empresa.

O Plano integra o programa de privacidade e proteção de dados da Perfur e deve ser interpretado em conjunto com a Política de Privacidade, a Política de Direitos do Titular de Dados e os demais procedimentos internos relacionados à segurança da informação e à proteção de dados.

O presente documento considera a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente seus arts. 46 e 48, e a regulamentação da Autoridade Nacional de Proteção de Dados (ANPD) aplicável aos incidentes de segurança, incluindo a Resolução CD/ANPD nº 15/2024.

#### 1. OBJETIVO

Este Plano tem por objetivo estabelecer uma resposta organizada, proporcional e documentada a incidentes de segurança que envolvam dados pessoais, buscando identificar rapidamente o ocorrido,

conter seus efeitos, reduzir riscos aos titulares, preservar evidências, adotar medidas corretivas e, quando cabível, realizar as comunicações exigidas pela legislação.

O PRI também estabelece responsabilidades mínimas para os colaboradores e responsáveis envolvidos, de modo que a Perfur possa atuar com transparência, prevenção, segurança e prestação de contas.

## 2. ABRANGÊNCIA E APLICAÇÃO

Este Plano aplica-se às atividades de tratamento de dados pessoais realizadas pela Perfur, independentemente do meio utilizado, físico ou eletrônico, e a todos os colaboradores, sócios, administradores, prestadores de serviços e terceiros que, em razão de suas atividades, tenham acesso a dados pessoais ou aos ambientes e documentos que os contenham.

A comunicação de uma suspeita de incidente não exige que o colaborador tenha certeza sobre a ocorrência. A avaliação, classificação e definição das providências caberão aos responsáveis designados pela Empresa.

## 3. O QUE É UM INCIDENTE DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS?

Para fins deste Plano, considera-se incidente de segurança qualquer evento adverso confirmado ou suspeito que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais, incluindo situações de destruição, perda, alteração, divulgação ou acesso não autorizado.

Podem constituir exemplos de incidentes:

- perda, extravio ou furto de documentos, computadores, dispositivos ou mídias que contenham dados pessoais;
- envio de e-mail, mensagem ou documento com dados pessoais ao destinatário incorreto;
- acesso, consulta, alteração, exclusão ou compartilhamento de dados pessoais sem autorização;
- phishing, malware, tentativa de invasão ou comprometimento de conta corporativa;
- indisponibilidade ou falha de sistema que impeça o acesso a dados pessoais ou comprometa sua integridade;
- divulgação indevida de dados pessoais em site, rede social, aplicativo, documento físico ou meio eletrônico;
- descarte inadequado de documentos ou mídias contendo dados pessoais;
- qualquer outra ocorrência acidental ou dolosa capaz de gerar risco à proteção dos dados pessoais.

## 4. PAPÉIS E RESPONSABILIDADES

### 4.1. Todos os colaboradores e prestadores

- comunicar imediatamente qualquer incidente ou suspeita de incidente pelo canal de privacidade indicado ao final deste documento;
- não apagar, alterar, encaminhar ou manipular evidências relacionadas ao incidente, salvo quando necessário para contenção imediata e segura;
- preservar o sigilo das informações a que tiver acesso durante a apuração;
- seguir as orientações da Empresa e participar de treinamentos e ações de conscientização sobre segurança e proteção de dados.

### 4.2. Encarregada pelo Tratamento de Dados Pessoais (DPO)

A Encarregada pelo Tratamento de Dados Pessoais da Perfur, Janaína Tiodolino Prado, será responsável por coordenar, conforme a estrutura interna da Empresa, a avaliação do incidente, a análise dos riscos aos titulares, a orientação das áreas envolvidas e, quando aplicável, a comunicação com a ANPD e com os titulares.

- receber ou acompanhar a comunicação interna do incidente;
- avaliar a natureza, extensão, categorias de dados e potenciais impactos aos titulares;
- coordenar as medidas de contenção, mitigação e prevenção, com apoio das áreas necessárias;
- avaliar a necessidade de comunicação à ANPD e aos titulares, observando a legislação e a regulamentação aplicáveis;
- manter o registro documental do incidente e das providências adotadas;
- acompanhar as medidas corretivas e as lições aprendidas após o encerramento do incidente.

### 4.3. Diretoria/gestão da Empresa

A administração da Perfur deverá apoiar a adoção das medidas necessárias à contenção e correção do incidente, disponibilizando recursos e acionando prestadores especializados quando a situação exigir suporte técnico, jurídico ou operacional.

### 4.4. Jurídico e prestadores especializados

Quando necessário, a Empresa poderá envolver assessoria jurídica, suporte de tecnologia da informação, fornecedores de sistemas ou outros prestadores especializados para investigar a causa, preservar evidências, corrigir vulnerabilidades e avaliar as consequências jurídicas e operacionais do incidente. O acesso às informações deverá ser limitado ao necessário.

## 5. DETECÇÃO E COMUNICAÇÃO DO INCIDENTE

A detecção poderá ocorrer por comunicação de colaborador, alerta de sistema, identificação de perda ou furto de documentos ou dispositivos, reclamação de titular, aviso de fornecedor, auditoria, rotina de verificação ou qualquer outra fonte confiável.

Ao tomar conhecimento ou suspeitar de um incidente, o colaborador deverá comunicar imediatamente a situação à Encarregada pelo Tratamento de Dados Pessoais pelo canal de privacidade indicado neste documento. Não é necessário aguardar a conclusão da apuração para realizar a comunicação.

Sempre que possível, o relato deverá informar:

- data e horário em que o fato foi percebido;
- como o incidente foi identificado;
- quais dados pessoais ou documentos podem estar envolvidos;
- quais pessoas, setores, sistemas ou fornecedores podem estar envolvidos;
- quais medidas já foram adotadas; e
- qualquer outra informação útil para a apuração.

A comunicação interna deve ser feita de forma restrita, evitando a divulgação do incidente a pessoas que não necessitem dessas informações para atuar na resposta.

## 6. AVALIAÇÃO, CLASSIFICAÇÃO E RESPOSTA

Após o recebimento da informação, a Perfur avaliará a ocorrência e definirá as medidas proporcionais ao risco. A avaliação deverá considerar, entre outros fatores, a natureza e a categoria dos dados, o número de titulares afetados, a possibilidade de identificação dos titulares, a extensão do incidente, a duração, os destinatários dos dados, a possibilidade de dano material ou moral e a existência de dados que demandem proteção reforçada.

| NÍVEL DE RESPOSTA | CRITÉRIOS E PROVIDÊNCIAS                                                                                                                                                                                                                                                                                                                                         |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Baixo             | Incidente limitado, com baixa probabilidade de causar impacto relevante aos titulares. Deve ser contido, registrado e avaliado para prevenção de recorrência.                                                                                                                                                                                                    |
| Médio             | Incidente com potencial de impacto significativo ou que exija atuação coordenada. Deve receber tratamento prioritário, com medidas de contenção, investigação, documentação e avaliação de eventual comunicação.                                                                                                                                                 |
| Alto              | Incidente que possa acarretar risco ou dano relevante aos titulares, especialmente quando envolver dados sensíveis, dados de crianças/adolescentes/idosos, dados financeiros, dados de autenticação, dados protegidos por sigilo ou dados em larga escala. Deve ser tratado com prioridade máxima e com avaliação imediata das comunicações legalmente exigidas. |

A classificação acima é operacional e não substitui os critérios legais para definir a obrigação de comunicação à ANPD e aos titulares. A decisão deverá considerar o caso concreto e a regulamentação vigente.

### 6.1. Medidas imediatas de contenção

- interromper, quando possível e seguro, o acesso ou fluxo que esteja provocando o incidente;
- bloquear ou alterar credenciais comprometidas;
- restringir acessos e permissões;
- recuperar ou recolher documentos e dispositivos, quando possível;

- corrigir destinatários ou configurações que tenham provocado exposição indevida;
- acionar suporte técnico ou fornecedor responsável pelo sistema, quando necessário;
- preservar registros e evidências relevantes para a investigação.

## 6.2. Investigação e correção

Após a contenção, a Empresa deverá buscar identificar a causa, a extensão e as consequências do incidente, registrando as providências adotadas. Quando aplicável, deverão ser implementadas medidas corretivas e preventivas, tais como revisão de permissões, alteração de senhas, atualização de sistemas, reforço de controles físicos, treinamento de colaboradores e revisão de procedimentos.

## 7. COMUNICAÇÃO À ANPD E AOS TITULARES

Nos termos da Resolução CD/ANPD nº 15/2024, a Perfur, na condição de controladora quando aplicável, deverá comunicar à ANPD e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A avaliação deverá considerar os critérios regulamentares, especialmente quando o incidente puder afetar significativamente interesses e direitos fundamentais e envolver, cumulativamente, ao menos uma das seguintes categorias: 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.

A comunicação à ANPD e aos titulares observará os prazos e condições da regulamentação vigente. Como regra geral, a Resolução CD/ANPD nº 15/2024 prevê comunicação em até 3 (três) dias úteis a partir do conhecimento, pelo controlador, de que o incidente afetou dados pessoais, ressalvadas as regras específicas aplicáveis aos agentes de tratamento de pequeno porte e eventual legislação específica.

Quando a Perfur estiver enquadrada como agente de tratamento de pequeno porte nos termos da regulamentação da ANPD, serão observadas as regras de prazo diferenciado previstas no Regulamento aplicável e na Resolução CD/ANPD nº 15/2024.

A comunicação aos titulares, quando exigida, deverá utilizar linguagem simples e de fácil compreensão e, quando possível, ser realizada de forma direta e individualizada. A comunicação deverá apresentar, no mínimo, as informações exigidas pela regulamentação da ANPD, incluindo a natureza e categoria dos dados afetados, riscos e possíveis impactos, medidas adotadas ou previstas e canal para obtenção de informações.

A comunicação à ANPD será realizada pelo procedimento e canal oficialmente disponibilizados pela Autoridade, pelo Encarregado ou por representante legalmente constituído, conforme a regulamentação vigente.

## 8. REGISTRO E DOCUMENTAÇÃO DO INCIDENTE

Todo incidente de segurança envolvendo dados pessoais deverá ser registrado e documentado, inclusive aqueles que não sejam comunicados à ANPD ou aos titulares, quando aplicável. O registro deverá permitir demonstrar as providências adotadas pela Empresa e subsidiar a prevenção de novos incidentes.

A Perfur manterá o registro dos incidentes pelo prazo mínimo de 5 (cinco) anos, contado da data do registro, salvo obrigações adicionais que exijam prazo maior, conforme a regulamentação aplicável.

O registro deverá conter, conforme aplicável:

- data de conhecimento do incidente e, quando possível, data de ocorrência;
- descrição geral das circunstâncias e causa, quando identificada;
- natureza e categorias dos dados afetados;
- número e categorias de titulares afetados;
- avaliação dos riscos e possíveis danos aos titulares;
- medidas de contenção, correção e mitigação;
- informações sobre eventual comunicação à ANPD e aos titulares; e
- justificativa para a ausência de comunicação, quando aplicável.

## 9. ENCERRAMENTO E PREVENÇÃO DE NOVOS INCIDENTES

Após a contenção e o tratamento do incidente, a Empresa deverá avaliar a necessidade de aperfeiçoamento de seus controles, políticas, contratos, treinamentos e medidas técnicas e organizacionais. Quando pertinente, as áreas envolvidas deverão participar de reunião de encerramento para registrar as lições aprendidas e definir ações preventivas.

As medidas adotadas deverão ser proporcionais aos riscos identificados e compatíveis com a natureza das operações de tratamento realizadas pela Perfur.

## 10. COMO FALAR COM A PERFUR SOBRE UM INCIDENTE?

Titulares, colaboradores, prestadores ou terceiros que identifiquem situação que possa envolver a segurança de dados pessoais poderão comunicar o fato à Perfur pelo canal de privacidade indicado abaixo.

| INFORMAÇÃO                                    | DADOS                                                                         |
|-----------------------------------------------|-------------------------------------------------------------------------------|
| Controlador                                   | Perfur do Brasil Ltda.                                                        |
| Encarregada pelo Tratamento de Dados Pessoais | Janaína Tiodolino Prado                                                       |
| E-mail para assuntos de privacidade/LGPD      | falaprotegida@perfur.com.br                                                   |
| Endereço para correspondências                | Avenida Assis Chateaubriand, nº 833, Independência, Taubaté/SP, CEP 12091-800 |

## 11. ALTERAÇÕES E DISPOSIÇÕES FINAIS

Este Plano poderá ser atualizado sempre que houver alteração relevante nas atividades de tratamento, na estrutura da Empresa, na legislação, na regulamentação da ANPD ou nos procedimentos internos de segurança e proteção de dados.

Em caso de dúvidas sobre a aplicação deste Plano, deverá ser consultada a Encarregada pelo Tratamento de Dados Pessoais. A versão vigente será disponibilizada no website da Perfur quando aplicável.

### CONTROLE DE VERSÃO

| VERSÃO | DATA       | DESCRIÇÃO                                                                                                                          |
|--------|------------|------------------------------------------------------------------------------------------------------------------------------------|
| 1.0    | 23/09/2026 | Adequação do Plano de Resposta a Incidentes de Segurança à realidade da Perfur do Brasil Ltda. e à regulamentação vigente da ANPD. |