



PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Procedimento operacional de governança LGPD

Campo	Informação
Versão	1.0
Data	17/09/2026
Status	PROCEDIMENTO OPERACIONAL VIGENTE
Documentos relacionados	Política Pública v2.2 RIPD v2.1 ROPA v2.1 Matriz de Consistência v1.1 DPA v1.1 Registro de Infraestrutura e Transferências Internacionais v1.0 Procedimento de Atendimento aos Titulares v1.0

Documento operacional destinado a orientar a identificação, contenção, avaliação, documentação, comunicação e tratamento de incidentes de segurança com dados pessoais no contexto dos Serviços FaceEye, preservando a regra geral segundo a qual o Cliente atua como Controlador e o FaceEye como Operador.

1. Objetivo e escopo

1.1. Este procedimento estabelece o fluxo de atuação do FaceEye diante de evento ou incidente de segurança que possa envolver dados pessoais tratados por meio da plataforma, desde o conhecimento inicial até o encerramento e registro do caso.

1.2. O procedimento abrange incidentes ocorridos no ambiente do FaceEye, em componentes sob sua gestão, durante atividades de suporte ou em Provedores de Infraestrutura e outros suboperadores que tratem dados pessoais no contexto dos Serviços, na medida em que o evento possa afetar dados tratados em nome de um Cliente.

1.3. Nem todo evento de segurança constitui incidente com dados pessoais, e nem todo incidente com dados pessoais exige comunicação à ANPD ou aos titulares. A classificação e a comunicação devem considerar os critérios legais e regulamentares aplicáveis ao caso concreto.

2. Papéis e princípio de atuação

- Cliente como Controlador: como regra geral, cabe ao Cliente avaliar o risco ou dano relevante e decidir e realizar as comunicações à ANPD e aos titulares quando legalmente exigidas.
- FaceEye como Operador: ao tomar conhecimento de incidente envolvendo dados tratados em nome de Cliente, o FaceEye deverá informar o Cliente sem demora injustificada e fornecer as informações disponíveis necessárias à avaliação e às comunicações cabíveis.
- Cooperação: FaceEye e Cliente deverão atuar de forma coordenada para conter o incidente, preservar informações pertinentes, mitigar efeitos e permitir o cumprimento dos prazos aplicáveis.

- **Proporcionalidade:** a resposta deverá considerar natureza, extensão, categorias de dados, quantidade e características dos titulares, possíveis consequências e medidas de contenção já adotadas.
- **Não transferência de responsabilidade:** a atuação técnica do FaceEye não substitui a responsabilidade do Cliente-Controlador pela comunicação regulatória e aos titulares.
- **Exceção:** quando o incidente envolver tratamento para finalidade própria e distinta em que o FaceEye excepcionalmente atue como Controlador, o FaceEye cumprirá diretamente as obrigações correspondentes nessa condição.

3. Conceitos operacionais

Conceito	Definição operacional
Evento de segurança	Ocorrência observada que possa demandar análise, mas que ainda não tenha sido confirmada como incidente envolvendo dados pessoais.
Incidente de segurança com dados pessoais	Evento confirmado que comprometa ou possa comprometer confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais tratados no contexto dos Serviços.
Risco ou dano relevante	Situação avaliada segundo os critérios da LGPD e da regulamentação da ANPD, considerando os dados, titulares, escala, impactos possíveis e demais circunstâncias do incidente.
Conhecimento do incidente	Momento em que existem elementos suficientes para concluir, de forma razoável, que ocorreu incidente de segurança afetando dados pessoais.
Contenção	Medidas destinadas a interromper, limitar ou reduzir a continuidade ou expansão dos efeitos do incidente.
Registro de incidente	Documentação específica do caso mantida para fins de governança, responsabilização e atendimento à regulamentação, não se confundindo com funcionalidade de logs da plataforma.

4. Gatilhos e origem do incidente

4.1. O fluxo poderá ser iniciado a partir de informação recebida de Cliente, usuário, titular, Provedor de Infraestrutura, outro fornecedor, profissional autorizado ou por constatação técnica durante a operação, suporte, manutenção ou diagnóstico.

4.2. A mera existência de vulnerabilidade não deve ser tratada automaticamente como incidente com dados pessoais. Quando houver indício de exploração, acesso indevido, perda, destruição, alteração, indisponibilidade ou divulgação não autorizada, deverá ser realizada análise para confirmar o evento e seu alcance.

5. Fluxo operacional de resposta

Etapas	Procedimento
1. Recebimento e registro	Registrar a data e hora do conhecimento disponível, origem da informação, sistemas ou ambientes potencialmente envolvidos e descrição inicial do evento.

Etapa	Procedimento
2. Triagem	Verificar se há indícios de envolvimento de dados pessoais, quais Clientes podem estar relacionados e se o FaceEye atua como Operador ou, excepcionalmente, como Controlador.
3. Contenção	Adotar medidas técnicas razoáveis e disponíveis para interromper ou limitar o evento e reduzir sua propagação, preservando a continuidade dos Serviços quando possível.
4. Apuração	Levantar natureza do evento, período estimado, dados e categorias afetadas, titulares potencialmente envolvidos, extensão, origem conhecida e medidas adotadas.
5. Avaliação preliminar	Organizar informações que permitam ao Cliente avaliar risco ou dano relevante, sem que o FaceEye substitua o juízo jurídico do Controlador.
6. Comunicação ao Cliente	Informar o Cliente sem demora injustificada, ainda que determinadas informações permaneçam em apuração, e complementar as informações à medida que forem confirmadas.
7. Cooperação	Fornecer ao Cliente elementos necessários para eventual comunicação à ANPD e aos titulares e apoiar tecnicamente medidas de mitigação.
8. Recuperação	Restabelecer os componentes afetados de forma segura e, quando cabível, utilizar os mecanismos de recuperação de desastre previstos para o ambiente.
9. Encerramento e registro	Consolidar fatos, medidas, comunicações, conclusão e ações corretivas pertinentes, preservando o registro do incidente pelo período aplicável.

6. Comunicação FaceEye → Cliente

6.1. Quando o FaceEye confirmar incidente de segurança envolvendo dados pessoais tratados em nome de um Cliente, deverá comunicar o fato ao Cliente sem demora injustificada. A comunicação inicial poderá ser preliminar quando ainda não houver informações completas.

6.2. Sempre que disponíveis e pertinentes, o FaceEye deverá informar: natureza do incidente; data ou período estimado; data do conhecimento; categorias de dados afetados; número ou estimativa de titulares; categorias de titulares; sistemas, Localidades ou ambientes envolvidos; possíveis consequências conhecidas; medidas de contenção e mitigação adotadas; e ponto de contato para acompanhamento.

6.3. Informações ainda não confirmadas deverão ser identificadas como preliminares. O FaceEye deverá complementar ou corrigir a comunicação quando novos elementos relevantes forem apurados.

7. Avaliação de risco ou dano relevante

7.1. A decisão sobre a necessidade de comunicação à ANPD e aos titulares cabe, como regra, ao Cliente-Controlador. O FaceEye fornecerá os elementos técnicos disponíveis para subsidiar essa avaliação.

7.2. A avaliação deverá considerar, entre outros fatores aplicáveis, se o incidente envolve dados pessoais sensíveis, dados de crianças, adolescentes ou idosos, dados financeiros, dados de autenticação,

dados sujeitos a sigilo ou tratamento em larga escala, bem como a possibilidade de danos materiais ou morais, discriminação, fraude, roubo de identidade, violação de imagem ou reputação e impedimento do exercício de direitos ou utilização de serviços.

7.3. Como o FaceEye trata dados biométricos utilizados para reconhecimento facial, incidentes que atinjam essas informações deverão receber avaliação especialmente cuidadosa por envolverem dados pessoais sensíveis.

8. Comunicação à ANPD e aos titulares

8.1. Nos termos da regulamentação vigente, quando o incidente puder acarretar risco ou dano relevante aos titulares, cabe ao Controlador comunicar a ocorrência à ANPD e aos titulares no prazo regulamentar aplicável. Na data desta versão, a Resolução CD/ANPD nº 15/2024 estabelece prazo de 3 (três) dias úteis, ressalvada a existência de prazo específico em outra legislação.

8.2. Quando o Cliente não dispuser de todas as informações necessárias dentro do prazo aplicável, poderá utilizar, quando cabível, comunicação preliminar e posterior complementação nos termos da regulamentação vigente. O FaceEye deverá cooperar para fornecer as informações técnicas sob seu domínio.

8.3. A comunicação aos titulares é responsabilidade do Cliente-Controlador e deverá observar forma, conteúdo e meios exigidos pela regulamentação. O FaceEye poderá fornecer informações técnicas necessárias à elaboração da comunicação, preservados segredos comercial e industrial.

8.4. O FaceEye não realizará comunicação em nome do Cliente à ANPD ou aos titulares sem autorização ou instrumento específico que legitime essa atuação, ressalvadas obrigações próprias que lhe sejam legalmente impostas.

9. Incidentes comunicados por Provedor de Infraestrutura ou suboperador

9.1. Quando o FaceEye receber de Provedor de Infraestrutura ou outro suboperador informação sobre incidente que possa afetar dados dos Clientes, deverá aplicar o mesmo fluxo de triagem, apuração e comunicação previsto neste procedimento.

9.2. A identidade do Provedor de Infraestrutura, a Região de Processamento e eventual transferência internacional não alteram a distribuição geral de papéis entre Cliente e FaceEye. Quando o incidente envolver infraestrutura localizada no exterior, deverão ser observados adicionalmente os instrumentos e requisitos aplicáveis ao fluxo internacional.

9.3. A resposta a incidente não depende da conclusão de eventual apuração de responsabilidade do fornecedor. A prioridade operacional é conter efeitos, obter informações suficientes e permitir ao Controlador cumprir suas obrigações.

10. Backup e recuperação de desastre

10.1. O backup do FaceEye destina-se exclusivamente à recuperação de desastre ou perda total do ambiente e não constitui mecanismo de recuperação individual de dados ou histórico de versões.

10.2. A restauração de backup somente deverá ser considerada quando tecnicamente necessária à recuperação do ambiente. O backup diário integral compreende aplicação, banco de dados e repositório de imagens; após a conclusão do novo ciclo, o backup anterior é removido, permanecendo somente o mais recente.

10.3. A existência de cópia em backup deverá ser considerada na análise de contenção e recuperação quando materialmente relacionada ao incidente, sem alterar as regras de retenção e substituição já definidas para esse mecanismo.

11. Preservação e registro do incidente

11.1. O FaceEye deverá manter registro documental dos incidentes de segurança com dados pessoais sob sua esfera de atuação, incluindo fatos conhecidos, efeitos, medidas técnicas e administrativas adotadas, comunicações realizadas e conclusão do caso, na medida aplicável ao seu papel.

11.2. Os registros exigidos pela regulamentação deverão ser preservados pelo prazo legal aplicável. Na data desta versão, a Resolução CD/ANPD nº 15/2024 estabelece período mínimo de 5 (cinco) anos para o registro dos incidentes de segurança com dados pessoais.

11.3. O registro de incidente é um documento de governança e responsabilização e não pressupõe a existência de recurso de logs ou trilha automatizada na plataforma FaceEye.

12. Matriz de responsabilidades

Atividade	Responsável principal
Detectar ou receber informação sobre evento no ambiente FaceEye	FaceEye, quando o evento estiver sob sua esfera técnica
Conter evento no ambiente sob gestão do FaceEye	FaceEye
Apurar elementos técnicos do incidente no FaceEye	FaceEye
Informar incidente ao Cliente sem demora injustificada	FaceEye
Avaliar risco ou dano relevante para titulares	Cliente-Controlador, com subsídios técnicos do FaceEye
Comunicar incidente à ANPD quando exigido	Cliente-Controlador
Comunicar titulares quando exigido	Cliente-Controlador
Fornecer informações técnicas para as comunicações	FaceEye
Executar medidas técnicas de mitigação na plataforma	FaceEye, dentro de sua esfera de atuação
Definir medidas de negócio e relacionamento com titulares	Cliente-Controlador
Manter registro regulatório do incidente	Cada agente na extensão das obrigações que lhe forem aplicáveis

13. Situações especiais

13.1. Incidente originado no ambiente do Cliente

Quando o incidente tiver origem em dispositivo, credencial, rede, integração, exportação ou outro recurso sob responsabilidade do Cliente, o Cliente deverá conduzir as medidas sob seu domínio e informar o FaceEye quando houver potencial impacto sobre a plataforma ou dados nela tratados. O FaceEye cooperará tecnicamente dentro do escopo dos Serviços.

13.2. Exportações em Excel ou PDF

Após a exportação de dados pelo Cliente, a guarda, compartilhamento e segurança do arquivo fora do ambiente FaceEye passam a integrar a governança do Cliente. Incidente restrito exclusivamente a

arquivo já exportado deverá ser conduzido pelo Cliente, sem prejuízo da cooperação do FaceEye quando necessária para identificar o conteúdo originalmente extraído.

13.3. Incidente envolvendo reconhecimento facial

Quando o incidente envolver Recortes Faciais, Representações Biométricas, referências biométricas ou outros dados sensíveis relacionados ao reconhecimento facial, essa circunstância deverá ser explicitamente considerada na avaliação de risco e nas medidas de mitigação.

13.4. Mais de um Cliente afetado

Quando um mesmo incidente afetar dados de mais de um Cliente, o FaceEye deverá preservar a segregação das informações e comunicar cada Controlador sobre o impacto pertinente ao seu ambiente, evitando exposição indevida de dados ou informações de outros Clientes.

14. Encerramento e ações posteriores

14.1. O incidente poderá ser encerrado operacionalmente quando houver elementos suficientes sobre causa conhecida ou provável, alcance, dados e Clientes afetados, medidas adotadas e pendências remanescentes, sem prejuízo de investigações ou obrigações posteriores.

14.2. Quando pertinente, o encerramento deverá identificar ações corretivas ou preventivas razoáveis, responsáveis e necessidade de revisão de procedimento, configuração, fornecedor ou medida técnica. A documentação de melhoria não deverá afirmar a existência de controle que ainda não tenha sido efetivamente implementado.

14.3. Alterações de Provedor de Infraestrutura ou Região de Processamento não exigem, por si só, revisão deste procedimento, salvo se modificarem materialmente o fluxo de resposta, as responsabilidades ou requisitos legais aplicáveis.

15. Gatilhos de revisão

- alteração relevante da LGPD ou da regulamentação da ANPD sobre incidentes de segurança;
- mudança material na arquitetura que altere o fluxo de resposta ou responsabilidades;
- incidente relevante que revele necessidade de aperfeiçoamento do procedimento;
- alteração contratual relevante entre FaceEye e Clientes ou suboperadores;
- implementação efetiva de novos controles que modifique as etapas aqui descritas.

16. Referências normativas

Lei nº 13.709/2018 (LGPD), especialmente arts. 46 a 49; Resolução CD/ANPD nº 15/2024 (Regulamento de Comunicação de Incidente de Segurança); e demais normas aplicáveis vigentes no momento do incidente.

17. Controle do documento

Campo	Registro
Documento	LGPD 8 - Procedimento de Resposta a Incidentes de Segurança
Versão	1.0
Data	17/09/2026
Responsável pela manutenção	FaceEye - governança de privacidade
Periodicidade de revisão	Quando houver gatilho de revisão ou mudança normativa relevante
Classificação	Uso interno / governança LGPD