

FaceEye

POLÍTICA DE CONTROLE DE ACESSO E SEGURANÇA

Governança de acesso e proteção dos dados pessoais

Campo	Informação
Versão	1.0
Data	17/09/2026
Status	POLÍTICA OPERACIONAL VIGENTE
Documentos relacionados	Política Pública v2.2 RIPD v2.1 ROPA v2.1 DPA v1.1 LGPD 7 v1.0 LGPD 8 v1.0 LGPD 9 v1.0

Documento operacional destinado a estabelecer as regras de controle de acesso e as medidas de segurança efetivamente adotadas no contexto da plataforma FaceEye, respeitando os papéis de Cliente-Controlador e FaceEye-Operador e evitando declarar controles tecnológicos que não estejam implementados.

1. Objetivo e escopo

1.1. Esta Política estabelece princípios, responsabilidades e procedimentos para concessão, administração, utilização e revogação de acessos à plataforma FaceEye e para proteção dos dados pessoais tratados no âmbito dos Serviços.

1.2. Aplica-se aos usuários administrados pelo Cliente, aos profissionais autorizados do FaceEye que necessitem de acesso para suporte, manutenção, diagnóstico ou continuidade dos Serviços e, quando pertinente, aos acessos técnicos associados a Provedores de Infraestrutura ou outros suboperadores.

1.3. As medidas descritas neste documento correspondem aos controles atualmente adotados ou às regras operacionais que devem reger sua utilização. A Política não deve ser interpretada como declaração de existência de funcionalidade ou controle técnico não expressamente identificado como implementado.

2. Papéis e princípios de atuação

- Cliente como Controlador: administra seus usuários, define os Perfis de Acesso e determina quais pessoas podem consultar ou operar os dados de seu ambiente.
- FaceEye como Operador: disponibiliza e opera os mecanismos de autenticação, autorização e segregação necessários à prestação dos Serviços, dentro das funcionalidades efetivamente implementadas.
- Menor acesso necessário: cada usuário deve receber somente as permissões necessárias às atividades que lhe tenham sido atribuídas.
- Segregação por Cliente: dados, Detecções, Localidades, Grupos e demais informações de um Cliente não devem ser disponibilizados a outros Clientes por meio das permissões ordinárias da plataforma.

- Responsabilidade compartilhada: o Cliente responde pela correta administração de seus usuários e permissões; o FaceEye responde pela operação dos mecanismos técnicos disponibilizados no Serviço.
- Segurança proporcional: as medidas técnicas e administrativas devem considerar natureza dos dados, contexto do tratamento, riscos e estado da tecnologia.

3. Conceitos operacionais

Conceito	Definição operacional
Usuário	Pessoa autorizada a acessar a plataforma mediante credencial individual.
Perfil de Acesso	Conjunto de permissões atribuído a um usuário para limitar funcionalidades e informações que poderá acessar ou operar.
Autenticação	Mecanismo utilizado para verificar a identidade declarada do usuário no acesso à plataforma.
Autorização	Aplicação das permissões associadas ao usuário ou ao seu Perfil de Acesso.
Segregação lógica	Separação lógica dos ambientes e informações de Clientes distintos de acordo com a arquitetura e as permissões do Serviço.
Acesso de suporte	Acesso realizado por profissional autorizado do FaceEye quando necessário à prestação de suporte, manutenção, diagnóstico ou continuidade dos Serviços.
Provedor de Infraestrutura	Prestador de recursos de computação, hospedagem, processamento, armazenamento ou serviços tecnológicos necessários à operação da plataforma.

4. Administração de usuários pelo Cliente

4.1. O Cliente é responsável pela criação, administração e desativação dos usuários vinculados ao seu ambiente, bem como pela atribuição dos Perfis de Acesso compatíveis com as funções de cada usuário.

4.2. O Cliente deverá restringir o acesso às pessoas efetivamente autorizadas e revisar usuários e permissões sempre que houver mudança de função, desligamento, substituição ou perda da necessidade de acesso.

4.3. Credenciais são individuais e não devem ser compartilhadas. O Cliente deverá orientar seus usuários a preservar a confidencialidade de suas credenciais e a comunicar suspeitas de comprometimento.

4.4. A disponibilização de perfis e permissões pelo FaceEye não substitui a responsabilidade do Cliente pela decisão de quem deve acessar os dados e para quais atividades.

5. Autenticação e autorização

- 5.1. O acesso ordinário à plataforma ocorre mediante autenticação individual, seguida da aplicação das permissões associadas ao usuário e ao respectivo Perfil de Acesso.
- 5.2. O FaceEye deverá manter os mecanismos de autenticação e autorização compatíveis com as funcionalidades efetivamente disponibilizadas e com a arquitetura vigente.
- 5.3. O Cliente deverá utilizar os recursos de controle de acesso disponibilizados de maneira coerente com suas necessidades e com a sensibilidade dos dados tratados.
- 5.4. Esta Política não declara a existência de mecanismos adicionais de autenticação ou de controles técnicos que não estejam efetivamente implementados na plataforma.

6. Perfis e permissões

- 6.1. Os Perfis de Acesso devem permitir que o Cliente diferencie, conforme as funcionalidades existentes, as permissões concedidas a seus usuários.
- 6.2. A atribuição de permissões deverá observar o princípio do menor acesso necessário e evitar concessões mais amplas do que as exigidas pela atividade do usuário.
- 6.3. O Cliente é responsável por definir e manter a correspondência entre função do usuário e permissões concedidas. O FaceEye não decide, em nome do Cliente, quem deve visualizar ou utilizar determinada informação.

7. Segregação entre Clientes

- 7.1. A arquitetura do FaceEye deve preservar a segregação lógica das informações pertencentes aos diferentes Clientes e impedir que as permissões ordinárias concedidas em um ambiente produzam acesso aos dados de outro Cliente.
- 7.2. A existência de mecanismos técnicos internos, inclusive Coleção, Person ID ou deduplicação de referências, não constitui autorização para consulta, reconhecimento, histórico ou utilização cruzada de dados entre Clientes.
- 7.3. O Person ID permanece chave técnica interna e não deve ser utilizado como mecanismo de compartilhamento de informações entre Clientes.

8. Acesso por profissionais do FaceEye

- 8.1. Profissionais autorizados do FaceEye poderão acessar dados existentes no ambiente do Cliente quando necessário à prestação de suporte, manutenção, diagnóstico ou continuidade dos Serviços.
- 8.2. O acesso deverá ocorrer no contexto da prestação dos Serviços e ser limitado às informações necessárias à atividade executada.
- 8.3. O FaceEye deverá restringir internamente a possibilidade de acesso aos profissionais cuja atividade possa demandá-lo e orientar essas pessoas quanto à confidencialidade e ao uso adequado das informações.
- 8.4. O atendimento de suporte não constitui finalidade autônoma para conservação de cópias dos dados pessoais. Os dados tratados durante o suporte permanecem sujeitos às regras de retenção aplicáveis aos dados de origem.

9. Dispositivos de captura

- 9.1. As Capturas são realizadas em tablets ou celulares pertencentes ao Cliente ou por ele administrados e associados a uma Localidade.
- 9.2. O Cliente é responsável pela administração física e operacional desses dispositivos, inclusive por restringir sua utilização a pessoas autorizadas e adotar cuidados compatíveis com o ambiente em que forem instalados ou utilizados.
- 9.3. A Captura original permanece no dispositivo e está sujeita à expiração automática prevista de 7 dias. O Recorte Facial produzido localmente é transmitido ao ambiente FaceEye para processamento.

10. Provedor de Infraestrutura e suboperadores

- 10.1. O FaceEye poderá utilizar Provedores de Infraestrutura e outros fornecedores necessários à prestação dos Serviços. Esses prestadores serão considerados suboperadores quando efetivamente realizarem tratamento de dados pessoais em nome da cadeia de tratamento.
- 10.2. A identidade do Provedor de Infraestrutura e a Região de Processamento são elementos técnicos variáveis e são tratados no registro operacional específico da suíte LGPD.
- 10.3. A alteração de provedor, arquitetura ou Região de Processamento não altera, por si só, os princípios de controle de acesso definidos nesta Política, sem prejuízo da avaliação de impactos materiais e das obrigações legais aplicáveis.

11. Proteção das informações e dever de confidencialidade

- 11.1. Dados pessoais acessados no contexto dos Serviços devem ser utilizados somente para as atividades autorizadas e não podem ser divulgados, copiados ou utilizados para finalidade incompatível com a prestação dos Serviços ou com as instruções do Cliente.
- 11.2. O FaceEye deverá adotar medidas técnicas e administrativas compatíveis com os riscos do tratamento para proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado.
- 11.3. Obrigações de confidencialidade e segurança permanecem aplicáveis às pessoas que intervenham no tratamento, inclusive após o término do acesso ou da atividade pertinente, na medida prevista em lei e nos instrumentos aplicáveis.

12. Mudanças, desligamentos e revogação de acesso

- 12.1. O Cliente deverá revogar ou adequar os acessos de seus usuários quando cessar a necessidade de utilização, houver desligamento ou ocorrer mudança de atribuições.
- 12.2. O FaceEye deverá revogar ou restringir acessos internos de profissionais quando cessar a necessidade relacionada às suas atividades.
- 12.3. Suspeita de comprometimento de credencial ou acesso indevido deverá ser tratada com prioridade, com alteração ou bloqueio do acesso quando tecnicamente cabível e encaminhamento ao procedimento de incidentes quando houver indício de comprometimento de dados pessoais.

13. Relação com incidentes de segurança

13.1. Evento que possa representar acesso não autorizado, perda, alteração, divulgação ou outro tratamento inadequado de dados pessoais deverá ser avaliado conforme o LGPD 8 - Procedimento de Resposta a Incidentes de Segurança.

13.2. Esta Política disciplina controles preventivos e de acesso. A investigação, avaliação de risco, comunicação ao Cliente e demais providências relativas a incidente seguem o procedimento específico.

14. Responsabilidades operacionais

Atividade	Responsabilidade principal	Observação
Criar e desativar usuários do Cliente	Cliente	Administração do ambiente do Cliente.
Definir Perfis de Acesso dos usuários	Cliente	Conforme função e necessidade de acesso.
Operar autenticação e autorização da plataforma	FaceEye	Nos limites das funcionalidades implementadas.
Preservar segregação lógica entre Clientes	FaceEye	Controle técnico da plataforma.
Proteger credenciais de usuários	Cliente e usuário	Inclui não compartilhar credenciais.
Autorizar acesso de suporte	FaceEye	Somente profissionais autorizados e quando necessário ao Serviço.
Administrar dispositivos de captura	Cliente	Dispositivos pertencentes ao Cliente ou por ele administrados.
Gerir controles de Provedor de Infraestrutura	FaceEye	Conforme contratos, arquitetura e responsabilidades aplicáveis.
Tratar suspeita de incidente	Cliente e/ou FaceEye	Conforme origem e LGPD 8.

15. Controles não declarados por este documento

15.1. Para assegurar que a documentação reflita o ambiente real, esta Política não deve ser interpretada como declaração de existência de controles, funcionalidades ou evidências técnicas que não estejam expressamente implementados e validados.

15.2. Novos controles de segurança poderão ser incorporados à plataforma ao longo do tempo. Sua inclusão na documentação LGPD ocorrerá após confirmação de sua efetiva implementação e quando forem materialmente relevantes para a descrição das medidas adotadas.

15.3. Recomendações gerais de segurança provenientes de autoridades, normas ou boas práticas servem como referência de governança, mas não devem ser convertidas em afirmações sobre a arquitetura do FaceEye sem validação técnica.

16. Revisão e evolução

16.1. Esta Política deverá ser revista quando houver alteração material nos mecanismos de autenticação, autorização, Perfis de Acesso, segregação, acesso de suporte, arquitetura ou outros controles de segurança relevantes para os dados pessoais.

16.2. Alterações meramente comerciais de fornecedor ou de Região de Processamento que não modifiquem materialmente os controles descritos não exigem, por si só, nova versão desta Política.

16.3. A adoção futura de novo controle técnico deverá ser documentada somente após sua implementação efetiva e validação operacional.

17. Referências de governança

17.1. Esta Política observa os princípios e deveres de segurança previstos na LGPD, especialmente a adoção de medidas técnicas e administrativas adequadas à proteção dos dados pessoais, e deve ser interpretada em conjunto com os demais documentos da suíte LGPD do FaceEye.

17.2. Orientações da ANPD sobre segurança da informação constituem referência de boas práticas e deverão ser consideradas de forma compatível com o porte, o contexto, os riscos e as características efetivas do tratamento.

18. Controle do documento

Campo	Registro
Documento	LGPD 10 - Política de Controle de Acesso e Segurança
Versão	1.0
Data	17/09/2026
Responsável pela manutenção	FaceEye - governança de privacidade e segurança
Periodicidade de revisão	Sempre que ocorrer gatilho da Seção 16 ou revisão periódica da suíte LGPD.
Status	POLÍTICA OPERACIONAL VIGENTE