RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO E CONFORMIDADE LEGAL

Sistema Central Impulse One

De:	O Patrício
Para:	Impulse One — Aceleradora de Negócios
Assunto:	Segurança da informação e conformidade legal do sistema Central Impulse One

Documento técnico-jurídico de demonstração das medidas de segurança da informação e de conformidade com a legislação brasileira de proteção de dados.

Impulse

Junho de 2026 · Versão 1.0

Documento confidencial

1. Apresentação e objetivo

O presente documento tem por finalidade descrever, de forma técnica e fundamentada, as medidas de segurança da informação adotadas pelo sistema de gestão Central Impulse One, bem como demonstrar a sua aderência aos princípios e exigências da legislação brasileira de proteção de dados pessoais — em especial a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014).

O objetivo é oferecer a clientes, parceiros e demais partes interessadas a segurança jurídica e técnica de que as informações corporativas e os dados pessoais armazenados no sistema são tratados em ambiente protegido, criptografado e em conformidade com as boas práticas de mercado e com a lei aplicável.

Importante: este documento descreve a arquitetura de segurança do sistema e as garantias contratuais e certificações de seus provedores de infraestrutura. As certificações citadas foram consultadas em fontes oficiais em junho de 2026; recomenda-se confirmar a versão vigente de cada certificação e dos respectivos termos contratuais no momento da contratação.

2. Sumário executivo

O Central Impulse One é uma aplicação web (software como serviço — SaaS) sustentada por dois provedores de infraestrutura de nuvem reconhecidos internacionalmente e auditados por terceiros independentes:

- **Vercel** — responsável pela hospedagem e entrega da aplicação web, com certificações SOC 2 Type 2 e ISO 27001:2022 e tráfego servido exclusivamente por HTTPS/TLS;
- **Supabase** — responsável pelo banco de dados (PostgreSQL), pela autenticação dos usuários e pelo armazenamento de arquivos, com certificações SOC 2 Type II e ISO 27001, criptografia AES-256 em repouso e disponibilidade de região no Brasil (São Paulo).

Em síntese, o sistema é seguro porque combina, em todas as camadas, criptografia da informação (em trânsito e em repouso), autenticação robusta de identidade, controle de acesso aos dados, rotinas de backup e recuperação, proteção contra ataques de rede e infraestrutura certificada — atendendo aos princípios de segurança e de prevenção exigidos pela LGPD (art. 6º, incisos VII e VIII) e ao dever de adoção de medidas técnicas e administrativas de proteção (art. 46).

3. Visão geral da arquitetura do sistema

A arquitetura do Central Impulse One foi concebida sob o princípio de segurança desde a concepção (security by design), separando claramente a camada de apresentação (aplicação web) da camada de dados (banco de dados gerenciado), e mantendo toda a comunicação entre o usuário e o sistema sob criptografia.

3.1. Camada de aplicação — Vercel

A interface do sistema é entregue ao usuário por meio da plataforma Vercel, especializada na hospedagem de aplicações web sobre uma rede de borda (edge) global e distribuída, com computação executada predominantemente sobre infraestrutura de nuvem da Amazon Web Services (AWS). Esse modelo proporciona alta disponibilidade, desempenho e isolamento do ambiente de produção.

3.2. Camada de dados, autenticação e arquivos — Supabase

As informações do sistema são armazenadas em um banco de dados PostgreSQL gerenciado pela Supabase. A mesma plataforma é responsável pela autenticação dos usuários (login com e-mail e senha) e pelo armazenamento de documentos e anexos de texto (briefings, formulários, PDFs e arquivos de documento), organizados em compartimentos de armazenamento (buckets) segregados por finalidade. Os **arquivos de mídia (fotos e vídeos) não são armazenados no sistema**: permanecem no serviço de armazenamento em nuvem (Drive) de titularidade da contratante, ao qual o sistema apenas vincula pastas e direciona links — cabendo à contratante a guarda, a segurança e o backup desses arquivos.

3.3. Comunicação criptografada (HTTPS/TLS)

Toda a comunicação entre o navegador do usuário e o sistema trafega exclusivamente por HTTPS, com criptografia TLS (Transport Layer Security). Isso significa que os dados não circulam em texto aberto pela internet: são cifrados de ponta a ponta entre o dispositivo do usuário e os servidores, impedindo a interceptação por terceiros.

4. Infraestrutura e fornecedores de nuvem

A segurança de um sistema em nuvem depende, em grande medida, da maturidade de segurança de seus provedores de infraestrutura. Ambos os fornecedores utilizados pelo Central Impulse One mantêm programas de segurança auditados por entidades independentes e disponibilizam certificações e instrumentos contratuais de proteção de dados.

4.1. Vercel — hospedagem da aplicação

- **Certificações:** atestação SOC 2 Type 2 (critérios de Segurança, Confidencialidade e Disponibilidade), certificação ISO/IEC 27001:2022 (auditada por terceiro independente) e conformidade PCI DSS v4.0.
- **Criptografia:** HTTPS obrigatório com TLS 1.2/1.3, redirecionamento automático de HTTP para HTTPS, cabeçalho HSTS e criptografia AES-256 dos dados em repouso.
- **Proteção de rede:** mitigação automática de ataques de negação de serviço (DDoS) nas camadas de rede e de aplicação, e Web Application Firewall (WAF) com regras de bloqueio, limitação de taxa e modo de defesa contra ataques.
- **Resiliência:** rede de borda global com roteamento automático para o ponto disponível mais próximo em caso de indisponibilidade regional, e rotinas de backup com replicação para recuperação de desastres.
- **Conformidade contratual:** disponibiliza Acordo de Tratamento de Dados (Data Processing Addendum — DPA) público, com Cláusulas Contratuais Padrão para transferências internacionais, em conformidade com o GDPR europeu.

4.2. Supabase — banco de dados, autenticação e arquivos

- **Certificações:** certificada SOC 2 Type II e ISO/IEC 27001, com controles auditados por terceiros.
- **Criptografia:** todos os dados são criptografados em repouso com AES-256 (incluindo banco, índices, registros de transação, backups e arquivos do Storage) e em trânsito por TLS. Informações especialmente sensíveis recebem ainda camada adicional de criptografia em nível de aplicação.
- **Infraestrutura e residência de dados:** hospedada sobre a Amazon Web Services (AWS), com possibilidade de provisionamento na região da América do Sul — São Paulo, Brasil (sa-east-1) —, permitindo manter os dados em território nacional.
- **Backups e recuperação:** backups diários automáticos, com retenção dos 7 (sete) dias mais recentes e restauração para o backup de qualquer um desses dias, sempre criptografados em repouso.
- **Conformidade contratual:** disponibiliza Acordo de Tratamento de Dados (DPA) formal, atuando como operador dos dados, e mantém Política de Privacidade pública.

O quadro a seguir resume as principais garantias de cada provedor:

Fornecedor	Função no sistema	Certificações e garantias de segurança
Vercel	Hospedagem e entrega da aplicação web (edge)	SOC 2 Type 2; ISO 27001:2022; PCI DSS v4.0; HTTPS/TLS obrigatório; HSTS; AES-256 em repouso; mitigação de DDoS e WAF; DPA com cláusulas contratuais padrão.
Supabase	Banco de dados PostgreSQL, autenticação e arquivos	SOC 2 Type II; ISO 27001; AES-256 em repouso; TLS em trânsito; backups diários com retenção de 7 dias; região no Brasil (São Paulo); autenticação gerenciada (senhas com hash) e DPA.

5. Camadas de segurança da informação

A proteção dos dados no Central Impulse One não depende de um único mecanismo, mas de múltiplas camadas complementares (defesa em profundidade), descritas a seguir.

5.1. Criptografia em trânsito

Toda a comunicação ocorre por HTTPS com TLS 1.2/1.3. As requisições em HTTP são automaticamente redirecionadas para HTTPS, e o cabeçalho de segurança HSTS instrui o navegador a utilizar somente conexões cifradas. Dessa forma, nenhum dado — credenciais, informações de clientes ou documentos — trafega de forma legível pela rede.

5.2. Criptografia em repouso

Os dados armazenados em disco são cifrados com o algoritmo AES-256, padrão de mercado para criptografia simétrica, fornecido pela infraestrutura de nuvem subjacente (AWS) e mantido ativo de forma permanente. A criptografia abrange o banco de dados, os backups e os arquivos enviados ao sistema.

5.3. Autenticação e gestão de identidade

O acesso ao sistema exige autenticação individual por e-mail e senha, gerida pelo serviço de autenticação da Supabase. As senhas nunca são armazenadas em texto aberto: são protegidas por função de hash criptográfico (bcrypt) com salt aleatório, de modo que sequer o operador da infraestrutura tem acesso à senha original. Cada sessão autenticada é representada por um token de acesso assinado criptograficamente (JSON Web Token — JWT), de curta duração e renovado automaticamente enquanto a sessão permanece ativa. A plataforma oferece, ainda, a possibilidade de autenticação multifator (MFA) para reforço das contas.

5.4. Controle de acesso aos dados

O controle de acesso apoia-se em três níveis complementares: (i) autenticação obrigatória para qualquer operação; (ii) segregação de funções na própria aplicação, com perfis de acesso distintos conforme o papel do usuário (por exemplo, restrição de informações financeiras e gerenciais a perfis de gestão); e (iii) o mecanismo nativo de Segurança em Nível de Linha (Row Level Security — RLS) do PostgreSQL, que permite restringir, no próprio banco de dados, quais registros cada usuário pode acessar. A aplicação utiliza, no lado do cliente, exclusivamente a chave pública de acesso (anon key), mantendo as credenciais privilegiadas restritas ao ambiente protegido.

5.5. Armazenamento de arquivos

Os documentos e anexos de texto são mantidos em compartimentos de armazenamento (buckets) segregados por finalidade, sujeitos à mesma criptografia em repouso e às políticas de acesso da plataforma. A organização por finalidade reduz a superfície de exposição e facilita a governança sobre o ciclo de vida dos arquivos. Os arquivos de mídia (fotos e vídeos) não integram esse armazenamento — residem no Drive próprio da contratante, que responde por sua guarda, segurança e backup; o sistema limita-se a vincular pastas e direcionar links a esse Drive.

5.6. Backups e continuidade do serviço

A resiliência é assegurada por rotinas automáticas de backup diário do banco de dados, com retenção dos 7 (sete) dias mais recentes, igualmente criptografadas, e pela replicação da infraestrutura em nuvem. Em caso de incidente, o sistema pode ser restaurado para o backup de qualquer um desses dias. Esses mecanismos protegem contra perda acidental de dados e viabilizam a recuperação, atendendo ao princípio da prevenção (LGPD, art. 6º, VIII).

5.7. Proteção de rede e da aplicação

Na camada de entrega, a plataforma de hospedagem aplica mitigação automática de ataques de negação de serviço (DDoS) e dispõe de Web Application Firewall (WAF), capaz de bloquear tráfego malicioso e limitar abusos antes que alcancem a aplicação.

6. Conformidade com a legislação brasileira

A arquitetura de segurança descrita acima não é apenas uma boa prática de mercado: ela materializa deveres legais previstos no ordenamento jurídico brasileiro. Nos termos da LGPD, os dados cadastrais de clientes e colaboradores armazenados no sistema (nome, e-mail, contatos, entre outros) constituem dados pessoais (art. 5º, I), e todas as operações de coleta, armazenamento e consulta configuram tratamento (art. 5º, X).

6.1. Papéis e responsabilidades

A empresa que utiliza o Central Impulse One e decide quais dados serão tratados e para quais finalidades é a controladora dos dados (art. 5º, VI). Os provedores de infraestrutura (Supabase e Vercel, e a AWS por detrás deles) atuam como operadores/suboperadores, tratando os dados em nome e segundo as instruções do controlador (art. 5º, VII). Essa cadeia de responsabilidade é formalizada pelos Acordos de Tratamento de Dados (DPA) disponibilizados por cada provedor.

6.2. Princípio da segurança e dever de proteção (LGPD)

O art. 6º, VII, da LGPD estabelece o princípio da segurança nos seguintes termos:

> *"VII — segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão."*

Esse dever é reforçado pelo art. 46, que exige a adoção de medidas técnicas e administrativas de segurança, observadas "desde a fase de concepção do produto ou do serviço até a sua execução" (§ 2º). As medidas descritas neste documento — criptografia em trânsito e em repouso, autenticação com hash de senha, controle de acesso e backups — constituem precisamente as medidas técnicas exigidas pelo dispositivo.

O art. 47, por sua vez, determina que a segurança da informação seja garantida "mesmo após o término do tratamento", fundamentando as políticas de retenção, confidencialidade e eliminação segura de dados. E o art. 49 exige que os próprios sistemas sejam "estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança" — requisito atendido pela escolha de provedores certificados (SOC 2 Type II e ISO 27001).

6.3. Comunicação de incidentes e a ANPD

O art. 48 da LGPD impõe ao controlador o dever de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) — autoridade competente criada pelo art. 55-A da Lei — e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. O monitoramento contínuo da infraestrutura e os registros de atividade (logs) das plataformas subsidiam a detecção e a resposta a eventuais incidentes, em apoio a esse dever legal.

6.4. Transferência internacional de dados (art. 33)

Por se tratar de infraestrutura em nuvem, parte do tratamento pode ocorrer em data centers localizados fora do Brasil, o que configura transferência internacional de dados, disciplinada pelo art. 33 da LGPD. Esse ponto é tratado de forma transparente neste documento:

- **Banco de dados (Supabase):** pode ser provisionado na região de São Paulo (Brasil), hipótese em que os dados permanecem em território nacional, eliminando a transferência internacional quanto ao armazenamento principal.
- **Hospedagem da aplicação (Vercel):** tem processamento primário nos Estados Unidos. A licitude dessa transferência ampara-se nas garantias contratuais oferecidas pelo provedor (cláusulas contratuais para transferência internacional, integradas ao DPA), na forma admitida pelo art. 33, II.

Observação de conformidade: a ANPD editou, em 2024, a Resolução CD/ANPD nº 19/2024, que aprova as cláusulas-padrão contratuais brasileiras para transferência internacional. Recomenda-se, na formalização dos contratos, alinhar os instrumentos dos provedores a esse marco regulatório e, quando aplicável, obter o consentimento específico e destacado do titular para o caráter internacional da operação (art. 33, VIII). A adoção da região de São Paulo para o banco de dados é a medida mais robusta para mitigar esse ponto.

6.5. Marco Civil da Internet e aplicação da lei brasileira

O Marco Civil da Internet (Lei nº 12.965/2014) assegura ao usuário a inviolabilidade e o sigilo de suas comunicações e dados armazenados (art. 7º), bem como o direito a informações claras sobre coleta e uso. De especial relevância, o art. 11 determina que, sempre que a coleta ou o tratamento ocorra em território nacional — ou os dados sejam de usuários no Brasil —, aplica-se obrigatoriamente a legislação brasileira, "ainda que as atividades sejam realizadas por pessoa jurídica sediada no exterior". Ou seja: mesmo com infraestrutura internacional, o sistema e a empresa permanecem integralmente sujeitos à lei brasileira e a este regime de proteção.

6.6. Padrões técnicos de segurança (Decreto nº 8.771/2016)

Como referência de boas práticas, o art. 13 do Decreto nº 8.771/2016 — que regulamenta o Marco Civil — elenca diretrizes de segurança que encontram correspondência direta nas medidas do sistema: controle estrito de acesso com privilégios por usuário; mecanismos de autenticação (inclusive autenticação dupla); registro/inventário de acessos; e uso de criptografia para garantir a inviolabilidade dos dados. Tais diretrizes são contempladas, respectivamente, pelo controle de acesso e segregação

de perfis, pela autenticação gerenciada com suporte a MFA, pelos registros de atividade das plataformas e pela criptografia TLS e AES-256.

O quadro a seguir relaciona os principais dispositivos legais às medidas concretas do sistema:

Dispositivo legal	Exigência	Como o Central Impulse One atende
LGPD, art. 6º, VII e VIII	Segurança e prevenção no tratamento de dados.	Criptografia em trânsito (TLS) e em repouso (AES-256), backups e monitoramento.
LGPD, art. 46	Medidas técnicas e administrativas, desde a concepção.	Arquitetura security by design sobre provedores certificados; autenticação e controle de acesso.
LGPD, art. 47	Segurança mesmo após o término do tratamento.	Políticas de confidencialidade, retenção e eliminação segura.
LGPD, art. 48	Comunicação de incidentes à ANPD e aos titulares.	Monitoramento e logs das plataformas como apoio à detecção e resposta.
LGPD, art. 49	Sistemas estruturados conforme requisitos de segurança.	Provedores com SOC 2 Type II e ISO 27001.
LGPD, art. 33	Transferência internacional apenas com garantias.	Região Brasil (São Paulo) para o banco; cláusulas contratuais (DPA) para a hospedagem.
Marco Civil, art. 11	Aplicação da lei brasileira mesmo com infra no exterior.	Conformidade integral com a legislação brasileira.
Decreto 8.771/16, art. 13	Controle de acesso, autenticação, registros e criptografia.	RLS e perfis; MFA disponível; logs; TLS e AES-256.

7. Hospedagem sob domínio próprio da Impulse

O sistema poderá ser disponibilizado sob domínio próprio da Impulse (por exemplo, app.impulse.com.br ou sistema.impulse.com.br), caso o domínio seja fornecido, sem prejuízo de qualquer medida de segurança aqui descrita. A plataforma de hospedagem provisiona automaticamente um certificado SSL/TLS para o domínio personalizado, após a validação dos registros de DNS, com renovação automática antes do vencimento. O tráfego entre os usuários e o sistema permanece criptografado, e a transição para o domínio próprio é transparente — reforçando, inclusive, a identidade institucional e a confiança percebida pelos usuários.

8. Responsabilidades, governança e boas práticas

A segurança de um sistema de informação é uma responsabilidade compartilhada entre o provedor de infraestrutura e o controlador dos dados. Enquanto Vercel e Supabase garantem a segurança da infraestrutura (criptografia, certificações, disponibilidade e proteção de rede), cabe à Impulse, como controladora, observar as boas práticas de governança que completam o ciclo de conformidade:

- Gestão criteriosa de credenciais e perfis de acesso, concedendo a cada usuário apenas os privilégios necessários (princípio do menor privilégio);
- Ativação de autenticação multifator (MFA) nas contas administrativas das plataformas;
- Manutenção de Política de Privacidade e Termos de Uso, informando titulares sobre coleta, finalidade e tratamento dos dados (Marco Civil, art. 7º, VIII);
- Definição de política de retenção e eliminação de dados, em especial no encerramento de contratos (LGPD, art. 47);
- Procedimento de resposta a incidentes, com fluxo de comunicação à ANPD e aos titulares (LGPD, art. 48);
- Indicação de Encarregado pelo Tratamento de Dados (DPO) e canal de atendimento aos titulares, conforme a estrutura da empresa;
- Gestão, segurança e backup do seu próprio Drive, onde residem os arquivos de mídia (fotos e vídeos), que ficam fora do escopo de armazenamento do sistema.

9. Conclusão

O sistema Central Impulse One foi construído sobre uma base de infraestrutura segura, auditada e juridicamente amparada. A combinação de criptografia integral da informação (em trânsito e em repouso), autenticação robusta, controle de acesso, backups, proteção de rede e provedores certificados internacionalmente (SOC 2 Type II e ISO 27001) confere ao sistema um nível de segurança compatível com as exigências da Lei Geral de Proteção de Dados e do Marco Civil da Internet.

Diante do exposto, conclui-se que é seguro e legalmente sustentável manter as informações corporativas e os dados pessoais sob a gestão do Central Impulse One, observadas pela controladora as boas práticas de governança indicadas neste documento. As medidas técnicas adotadas atendem ao princípio da segurança (LGPD, art. 6º, VII) e ao dever de proteção (art. 46), e a estrutura permanece integralmente submetida à legislação brasileira (Marco Civil, art. 11).

10. Fontes oficiais consultadas

As informações técnicas e de conformidade deste documento foram consultadas, em junho de 2026, nas seguintes fontes oficiais:

- Lei nº 13.709/2018 (LGPD) — planalto.gov.br
- Lei nº 12.965/2014 (Marco Civil da Internet) — planalto.gov.br
- Decreto nº 8.771/2016 — planalto.gov.br
- Resolução CD/ANPD nº 19/2024 (cláusulas-padrão contratuais) — gov.br/anpd
- Central de Segurança e Conformidade da Vercel — vercel.com/docs/security
- Acordo de Tratamento de Dados (DPA) da Vercel — vercel.com/legal/dpa
- Central de Segurança da Supabase — supabase.com/security
- Documentação de regiões e backups da Supabase — supabase.com/docs

---

Nota metodológica: este documento descreve a arquitetura de segurança do sistema e as garantias dos provedores de infraestrutura, com base em fontes oficiais consultadas em junho de 2026. As certificações e os termos contratuais devem ser confirmados em sua versão vigente no momento da contratação. A efetividade das medidas depende, ainda, da correta configuração e da observância, pela controladora, das boas práticas de governança aqui indicadas.