Smart Process S.A.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 15 | 24 de fevereiro de 2026

Código do Documento	PSI-UPFLUX-v15
Versão	15
Data de Homologação	24/02/2026
Próxima Revisão	24/08/2026 (ciclo semestral)
Classificação	Confidencial – Distribuição Restrita
Responsável	Cleiton Garcia – DPO / Encarregado LGPD
E-mail DPO	dpo@upflux.net
Aprovadores	CSI (Comitê de Segurança da Informação) + Diretoria Executiva

CSG FK helt DD

Sumário

CSG FK helt DD

1 Introdução

1.1 Apresentação

A UpFlux Process Intelligence Ltda. (doravante “UpFlux”) é uma empresa brasileira especializada em Process Mining e Process Intelligence, reconhecida no Gartner Magic Quadrant 2024. Atuando no segmento SaaS B2B, a empresa fornece soluções analíticas para hospitais, cooperativas de saúde, indústrias e grandes organizações com operações de Procure-to-Pay (P2P) e Order-to-Cash (O2C), com integrações nativas a TOTVS, SAP e Sankhya.

A presente Política de Segurança da Informação (PSI) estabelece os princípios, diretrizes e responsabilidades para proteção das informações geridas pela UpFlux, garantindo a confidencialidade, integridade e disponibilidade dos dados de clientes, colaboradores e parceiros, em conformidade com a LGPD (Lei nº 13.709/2018), ISO/IEC 27001:2022 e demais regulamentos aplicáveis.

1.2 Objetivos

- Proteger os ativos de informação da UpFlux contra ameaças internas e externas;
- Assegurar conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e regulamentações ANS aplicáveis ao setor de saúde;
- Garantir a continuidade dos negócios e a resiliência operacional;
- Estabelecer padrões de conduta para colaboradores, terceiros e prestadores de serviços;
- Adotar os referenciais ABNT NBR ISO/IEC 27001:2022 e NIST Cybersecurity Framework como modelos de controles e gestão de riscos.

1.3 Declaração da Administração

A Diretoria Executiva da UpFlux declara seu comprometimento irrestrito com a segurança da informação, destinando recursos humanos, financeiros e tecnológicos para implementação e manutenção dos controles descritos nesta política. O cumprimento das diretrizes aqui estabelecidas é obrigatório para todos os colaboradores, prestadores de serviço e parceiros que acessem sistemas ou dados da UpFlux.

A Carta de Comprometimento da Alta Direção, assinada eletronicamente pelo representante legal, é parte integrante do presente documento (LGPD-CARTA-v2).

1.4 Escopo

Esta política se aplica a:

- Todos os colaboradores da UpFlux (CLT, PJ e estágiários);
- Prestadores de serviço e fornecedores com acesso a sistemas ou dados da empresa;
- Ativos de informação: sistemas, equipamentos, dados, documentos e infraestrutura tecnológica;
- Ambientes de produção, homologação e desenvolvimento hospedados na AWS (região us-east-2 – Ohio);
- Ambiente local (on-premises) da sede administrativa, protegido pelo firewall Fortinet FortiGate 60F.

1.5 Conceitos e Definições

Ativo de Informação: qualquer dado, sistema, equipamento ou documento com valor para a organização.

Titular de Dados: pessoa natural a quem se referem os dados pessoais tratados (art. 5º, LGPD).

DPO/Encarregado: Encarregado pelo Tratamento de Dados Pessoais, conforme art. 41 da LGPD.

CSI: Comitê de Segurança da Informação da UpFlux.

Incidente de Segurança: evento adverso que comprometa a confidencialidade, integridade ou disponibilidade de informações.

PAM (Privileged Access Management): conjunto de controles para gestão e auditoria de acessos privilegiados.

1.6 Documentos Relacionados

- Política de Privacidade e Proteção de Dados (ADOC-LGPD-v02)
- Política de Coleta Mínima de Dados e Consentimento Informado
- Política de Classificação e Manuseio da Informação (PCI v1.1)

CSG FK helt DD

- Política de Senhas e Autenticação
- Política de Desenvolvimento Seguro – DevSecOps (PS-SEC-DEVSECOPS v1.1 – 06/02/2026)
- Política de Gestão de Incidentes de Segurança da Informação
- Política de Retenção, Imutabilidade e Disponibilização de Logs (POL-SI-LOG-001 v1.1 – 06/02/2026)
- Política de Anonimização e Pseudonimização de Dados
- Política de Privacidade – Privacy by Design / Privacy by Default
- Política de Relatório de Impacto à Proteção de Dados (RIPD/DPIA)
- Política de Segurança de Servidores
- Plano de Continuidade de Negócios (PCN)
- Plano de Recuperação de Desastres (DRP)
- Acordos Gerais de Privacidade e Proteção de Dados (modelos contratuais)
- Carta de Comprometimento da Alta Direção – LGPD (LGPD-CARTA-v2)

1.7 Autores

Esta política foi elaborada pelo Comitê de Segurança da Informação (CSI) da UpFlux, com participação do DPO, da área de DevSecOps e da Diretoria Executiva.

1.8 Divulgação e Distribuição

Esta política é de ciência obrigatória para todos os colaboradores e está disponível na intranet corporativa. Versão resumida pode ser disponibilizada a clientes e parceiros mediante solicitação formal. A distribuição do documento completo a terceiros depende de autorização do CSI.

1.9 Versão e Revisão

Esta política é revisada a cada 6 (seis) meses ou imediatamente após: incidente de segurança relevante; mudança significativa de infraestrutura ou modelo de negócio; alteração regulatória (LGPD, ANS, ANPD). A próxima revisão programática está agendada para 24/08/2026.

1.10 Manutenção da Segurança da Informação

1.10.1 Comitê de Segurança da Informação (CSI)

O CSI é o órgão colegiado responsável pela governança de segurança da informação. Suas atribuições incluem: aprovar políticas, avaliar riscos, monitorar indicadores e coordenar a resposta a incidentes. Compositão e reuniões detalhadas no Anexo I. Reuniões ordinárias trimestrais e extraordinárias conforme demanda.

1.10.2 Inventário de Ativos

A UpFlux mantém inventário formal e atualizado de todos os ativos de informação por meio da ferramenta GLPI. O inventário abrange hardware (estações de trabalho, servidores físicos, equipamentos de rede), software licenciado, ativos em nuvem (recursos AWS) e documentos críticos. Cada ativo possui Dono de Ativo (Asset Owner) formalmente designado, responsável pela classificação e proteção adequadas, conforme PCI v1.1. O inventário é atualizado trimestralmente e sempre que houver movimentação relevante de ativos.

1.10.3 Gestão de Riscos

Os riscos de segurança são avaliados periodicamente pelo CSI com base no framework NIST CSF, contemplando: identificação de ameaças, avaliação de vulnerabilidades, análise de impacto e definição de controles. O resultado alimenta o Plano de Tratamento de Riscos (PTR), revisado semestralmente.

1.10.4 Conformidade Regulatória

A UpFlux opera em conformidade com: LGPD – Lei nº 13.709/2018 (DPO: Cleiton Garcia | dpo@upflux.net); regulamentações ANS aplicáveis em contextos de saúde; ABNT NBR ISO/IEC 27001:2022 e NIST Cybersecurity Framework como referenciais de controles e gestão.

1.10.5 Treinamento e Conscientização

Todos os colaboradores passam por treinamento de segurança da informação na admissão e anualmente. Campanhas adicionais são realizadas após incidentes relevantes ou atualizações desta política.

CSG FK helt DD

CSG FK helt DD

2 Segurança Cibernética

2.1 Autenticação e Controle de Acesso

2.1.1 Política Geral de Acesso

a) O acesso a sistemas e dados da UpFlux é concedido com base no princípio do menor privilégio (least privilege);
b) Contas de acesso são individuais e intransferíveis;
c) O provisionamento de acessos é formalizado pelo gestor responsável e aprovado pelo setor de TI;
d) Revisões de acessos (access review) são realizadas trimestralmente;
e) No desligamento de colaboradores, todos os acessos são revogados em até 24 horas após comunicação formal do RH.

2.1.2 Autenticação Multifator (MFA)

O uso de MFA é obrigatório em todos os sistemas que suportam essa funcionalidade, incluindo: e-mail corporativo (Microsoft 365), VPN, console AWS, ferramentas DevOps e painéis administrativos. A ativação é imposta automaticamente após o primeiro acesso do colaborador.

2.1.3 Gestão de Credenciais Privilegiadas (PAM)

A UpFlux adota os seguintes controles para gestão de acessos privilegiados:

- Cofre de senhas corporativo (Bitwarden): todas as senhas institucionais e segredos de serviço são gerenciados no Bitwarden, ferramenta homologada pelo CSI. O acesso ao cofre é controlado por MFA e auditado;
- Identidades gerenciadas na AWS: workloads em produção utilizam IAM Roles com permissões baseadas em menor privilégio. Não são utilizadas credenciais estáticas (access keys) em produção;
- Acesso interativo restrito: servidores e containers em produção não possuem usuários locais ou acesso SSH habilitado. Todas as interações ocorrem via pipelines CI/CD controlados;
- Segredos no pipeline: credenciais sensíveis são injetadas temporariamente no processo de build e não são armazenadas na imagem final;
- Acesso de emergência (break-glass): procedimento formal com notificação automática ao CSI e registro de auditoria.

2.2 Proteção de Endpoints

f) Todos os endpoints corporativos possuem solução EDR implantada: Bitdefender GravityZone Enterprise, com cobertura de 100% dos dispositivos gerenciados;
g) Atualização de assinaturas: automática, janela máxima de 24 horas;
h) Varreduras agendadas: a cada 5 dias em todos os endpoints;
i) Feeds de Threat Intelligence: integrados ao GravityZone e ao SIEM Elastic para detecção baseada em IOCs atualizados;
j) Alertas de detecção encaminhados automaticamente ao time de segurança via integração com o Elastic;
k) Dispositivos não gerenciados (BYOD) não são autorizados para acesso a sistemas corporativos sem aprovação formal do CSI.

2.3 Firewall e Proteção de Perímetro

l) Ambiente local (on-premises): Fortinet FortiGate 60F com regras baseadas em menor privilégio de rede, inspeção de conteúdo e IDS/IPS ativo;
m) Ambiente cloud (AWS Ohio – us-east-2): proteção via Security Groups, Network ACLs e WAF (Web Application Firewall). Regras de entrada restritas ao mínimo necessário;
n) Toda configuração de rede é gerenciada como Infraestrutura como Código (IaC), auditada por pipeline CI/CD.

2.4 Testes de Intrusão (Pentest)

o) Pentest externo e interno: semestral (março e setembro), por empresa especializada independente;
p) Após cada pentest, um Plano de Ação com prazos e responsáveis é formalizado pelo CSI;
q) Vulnerabilidades críticas: remediadas em até 2 dias úteis;

CSG FK helt DD

r) Relatórios classificados como Restritos; disponíveis a clientes mediante NDA.

2.5 Gestão de Vulnerabilidades e Atualizações

s) Varredura automática de vulnerabilidades: a cada 5 dias em toda a infraestrutura (endpoints, servidores, containers, AWS);
t) Gestão de patches por criticidade: CVSS ≥ 9.0 em 2 dias; CVSS 7.0-8.9 em 14 dias; CVSS 4.0-6.9 em 30 dias; CVSS < 4.0 conforme cronograma;
u) Análise de composição de software (SCA): integrada ao pipeline CI/CD para detecção de dependências com CVEs conhecidos;
v) Imagens de container reconstruídas periodicamente para incorporar correções de segurança.

2.6 Criptografia e Gestão de Chaves

w) Dados em repouso: AES-256 em todos os ambientes (RDS, S3, EBS);
x) Dados em trânsito: TLS 1.2 ou superior em todas as comunicações;
y) Gestão de chaves: AWS KMS com rotação automática e controle via IAM;
z) Segredos e credenciais: gerenciados no Bitwarden (cofre corporativo) e/ou AWS Secrets Manager. Veda-se armazenamento em código-fonte ou arquivos de configuração em texto claro;
aa) Algoritmos obsoletos (MD5, SHA-1, DES, SSL 3.0, TLS 1.0) são expressamente vedados.

2.7 Prevenção de Vazamento de Dados (DLP)

bb) Controles de DLP aplicados para evitar transferência não autorizada de informações Confidenciais e Restritas (conforme PCI v1.1);
cc) Vedado o armazenamento de dados confidenciais em dispositivos pessoais ou serviços de nuvem não homologados;
dd) Envio de dados de clientes por canais não criptografados ou não corporativos é expressamente proibido.

2.8 Rastreabilidade e Monitoramento

2.8.1 SIEM e Monitoramento Cloud (AWS)

A UpFlux mantém rastreabilidade completa por meio de:

- Elastic Security (SIEM): centralização, correlação e análise de logs de aplicação e infraestrutura. Integrado a AWS CloudTrail, GuardDuty e CloudWatch;
- AWS CloudTrail: auditoria de todas as ações na conta AWS (API calls, acesso ao console, alterações de configuração);
- AWS GuardDuty: detecção de ameaças e comportamentos anômalos na infraestrutura AWS;
- Amazon CloudWatch: monitoramento de métricas operacionais e alertas de performance;
- Fortinet FortiGate 60F: logs de firewall, IDS/IPS e tráfego de rede do ambiente local.

2.8.2 Retenção de Logs

Os logs são retidos conforme Política de Retenção, Imutabilidade e Disponibilização de Logs (POL-SI-LOG-001 v1.1), com proteção WORM contra alteração indevida e disponibilidade para auditorias e investigações.

2.8.3 Threat Intelligence

Feeds de inteligência de ameaças (Threat Intelligence) são integrados ao Elastic Security e ao Bitdefender GravityZone, permitindo detecção baseada em IOCs (Indicadores de Comprometimento) continuamente atualizados.

CSG FK helt DD

3 Segurança Lógica

3.1 Acesso à Internet

ee) O acesso à internet deve ocorrer pela conexão corporativa, com monitoramento e filtragem de conteúdo;

ff) Download ou execução de softwares não homologados pelo TI é expressamente proibido.

3.2 Acesso à Rede Corporativa

gg) Acesso remoto exclusivamente via VPN corporativa com MFA obrigatório;

hh) Dispositivos sem o agente EDR instalado e atualizado não serão autorizados na rede corporativa;

ii) Autenticação via Microsoft Entra ID (Azure AD), OpenID Connect e protocolos seguros homologados.

3.3 Armazenamento e Manuseio de Informações

3.3.1 Classificação da Informação

Toda informação deve ser classificada conforme a PCI v1.1 nos níveis: Pública, Interna, Confidencial e Restrita.

3.3.2 Armazenamento Autorizado

Informações Confidenciais e Restritas devem ser armazenadas exclusivamente em sistemas homologados. É vedado o uso de dispositivos pessoais, nuvens não corporativas ou mídias removentes não gerenciadas.

3.3.3 Transmissão

Toda transmissão de informações Confidenciais/Restritas deve utilizar canais criptografados (TLS 1.2+). É vedado o envio por e-mail pessoal ou canais não corporativos.

3.3.4 Infraestrutura de Produção

A infraestrutura de produção está hospedada integralmente na Amazon Web Services (AWS), região us-east-2 (Ohio, EUA). Componentes principais:

- Banco de dados: Amazon RDS (us-east-2), AES-256 em repouso e TLS em trânsito;
- Armazenamento: Amazon S3 com criptografia SSE-S3/SSE-KMS;
- Processamento: containers orquestrados via pipeline CI/CD;
- Gestão de chaves: AWS KMS com rotação automática;
- Monitoramento: AWS CloudTrail, GuardDuty, CloudWatch e Elastic (SIEM).

3.3.5 Backup e Recuperação

Política de backup em três camadas de retenção:

- Incremental: a cada 6 horas;
- Semanal: retido por 30 dias;
- Mensal: retido por 6 meses.

Todos os backups são criptografados na AWS. Testes de restauração realizados periodicamente. Objetivos de recuperação (conforme DRP): RPO de até 4 horas; RTO de até 8 horas.

3.3.6 Retenção e Descarte de Dados de Clientes

Após encerramento de contrato, os dados do cliente são mantidos por até 90 (noventa) dias, conforme Cláusula 3.2 dos Acordos Gerais de Privacidade e Proteção de Dados, após o que são definitivamente excluídos de todos os ambientes. O cliente pode solicitar exportação de seus dados antes do descarte. O descarte impede recuperação das informações.

3.4 Propriedade Intelectual

jj) Código-fonte, documentação e desenvolvimentos realizados na UpFlux são de propriedade exclusiva da empresa;

kk) Vedada a reprodução de softwares sem licença válida;

CSG FK helt DD

ll) Uso de bibliotecas open source deve ser avaliado quanto à compatibilidade de licença e vulnerabilidades, via processo SCA (DevSecOps).

3.5 Uso de Sistemas Corporativos

mm) Sistemas corporativos exclusivamente para finalidades profissionais;
nn) Toda instalação de software em dispositivos corporativos requer aprovação do TI;
oo) Acesso a sistemas de clientes limitado ao mínimo necessário, registrado e justificado.

3.6 Uso de E-mails

pp) E-mail corporativo exclusivamente para comunicações profissionais;
qq) Informações Confidenciais/Restritas devem ser enviadas via canais criptografados ou plataformas autorizadas;
rr) Vedado o encaminhamento de e-mails corporativos para contas pessoais;
ss) Acesso a e-mail pessoal em dispositivos corporativos durante o expediente não é permitido.

3.7 Uso de Senhas

3.7.1 Diretrizes gerais

tt) Senha pessoal e intransferível; colaborador responsável por ações realizadas com suas credenciais;
uu) Senhas não devem ser compartilhadas sob nenhuma circunstância;
vv) Complexidade mínima: 8 caracteres, com maiúsculas, minúsculas, números e caracteres especiais;
ww) Proibido reuso das últimas 3 versões de senha;
xx) Armazenamento obrigatório no cofre corporativo Bitwarden. Vedado registro em arquivos não criptografados;
yy) Bloqueio de conta após 5 tentativas de acesso inválidas consecutivas;
zz) Senhas temporárias substituídas no primeiro acesso.

3.7.2 Senhas institucionais

aaa) Todas as senhas institucionais com responsável formalmente definido e armazenadas no Bitwarden corporativo;
bbb) Senhas alteradas sempre que colaborador com acesso for transferido ou desligado.

3.8 Software de Mensagens Instantâneas

ccc) Somente Microsoft Teams é homologado para comunicações corporativas;
ddd) Aplicações pessoais (WhatsApp, Telegram) não devem ser usadas para comunicações que envolvam informações confidenciais.

3.9 Gerenciamento de Partes Externas

eee) Prestadores de serviço devem assinar NDA antes de receber qualquer acesso;
fff) Acesso de terceiros provisionado com mínimo de privilégio, prazo definido e monitorado;
ggg) Contratos devem incluir cláusulas de segurança e proteção de dados conforme Acordos Gerais de Privacidade.

3.10 Segurança Física

hhh) Acesso físico às instalações controlado e monitorado;
iii) Equipamentos corporativos não deixados sem supervisão em locais públicos;
jjj) Bloqueio automático de tela ativo em todos os dispositivos.

3.11 Controle de Equipamentos

kkk) Todo equipamento corporativo registrado no GLPI antes de ser colocado em uso;
lll) Movimentação, substituição ou descarte comunicados ao TI para atualização do inventário e descarte seguro.

CSG FK helt DD

3.12 Controle de Documentos Físicos

mmm) Documentos físicos Confidenciais/Restritos armazenados em local trancado;

nnn) Descarte com fragmentadora de papel ou serviço de descarte seguro certificado.

CSG FK helt DD

4 Políticas de Processos Internos

4.1 Desenvolvimento Seguro (DevSecOps)

A UpFlux adota abordagem DevSecOps, integrando segurança em todas as fases do SDLC, conforme Política de Desenvolvimento Seguro (PS-SEC-DEVSECOPS v1.1, vigor 06/02/2026). Controles mínimos por fase:

- Planejamento: Modelagem de Ameaças (Threat Modeling);
- Desenvolvimento: IDE Security Plugins (alertas de código inseguro em tempo real);
- Build/CI: SAST (análise estática) + SCA (dependências de terceiros);
- Testes: DAST (análise dinâmica) em homologação;
- Deploy/CD: validação de IaC com auditoria de configurações;
- Operação: monitoramento contínuo via Elastic SIEM e logs auditados.

Todas as mudanças em produção passam por fluxo controlado de revisão e aprovação no pipeline CI/CD, com rastreabilidade completa.

4.2 Gestão de Incidentes de Segurança

A UpFlux mantém processo formal de gestão de incidentes conforme Política de Gestão de Incidentes de Segurança da Informação. Incidentes são classificados por severidade e tratados dentro de SLAs definidos. Incidentes com possível impacto a dados pessoais são comunicados ao DPO, que avalia a necessidade de notificação à ANPD e/ou titulares, conforme art. 48 da LGPD.

4.3 Continuidade de Negócios e DRP

A UpFlux mantém Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP) ativos, testados anualmente. Objetivos: RPO até 4 horas; RTO até 8 horas.

4.4 Gestão de Fornecedores e Terceiros

A contratação de fornecedores que acessarão dados ou sistemas exige: avaliação de segurança prévia, assinatura de NDA/DPA, cláusulas de segurança no contrato e monitoramento do acesso. Fornecedores que atuam como operadores de dados pessoais estão sujeitos às obrigações da LGPD.

4.5 Privacidade e Proteção de Dados (LGPD)

A UpFlux está comprometida com os princípios da LGPD (Lei nº 13.709/2018), adotando Privacy by Design e Privacy by Default em todos os produtos e processos. DPO: Cleiton Garcia | dpo@upflux.net. O tratamento de dados pessoais ocorre com base legal definida, finalidade específica e minimização. O Registro de Atividades de Tratamento (RAT) é mantido atualizado pelo DPO.

4.6 Auditoria e Conformidade

Auditorias internas de segurança realizadas anualmente pelo CSI. Clientes enterprise e órgãos reguladores podem solicitar auditoria mediante acordo formal. Evidências de conformidade disponíveis sob demanda, respeitadas as classificações de sigilo.

CSG FK helt DD

5 Medidas Disciplinares

O descumprimento das diretrizes desta PSI sujeita o infrator a medidas proporcionais à gravidade da violação:

- Advertência formal;
- Suspensão do acesso aos sistemas até regularização;
- Medidas disciplinares administrativas, incluindo demissão por justa causa;
- Rescisão contratual imediata para prestadores de serviço;
- Responsabilização civil e/ou criminal nos termos da legislação brasileira aplicável, incluindo a LGPD.

A aplicação de medidas disciplinares é responsabilidade do CSI com a Diretoria Executiva e, quando aplicável, o setor jurídico. A UpFlux reserva-se o direito de acionar autoridades competentes (Polícia Federal, ANPD, Ministério Público) diante de evidências de crimes cibernéticos ou violações à LGPD.

CSG FK helt DD

Anexo I – Comitê de Segurança da Informação (CSI)

Reuniões ordinárias: trimestrais. Reuniões extraordinárias: convocadas em caso de incidentes relevantes.

Membro	Cargo / Função	Responsabilidade no CSI
Cleiton Garcia	DPO / Encarregado LGPD	Presidente do CSI | LGPD | dpo@upflux.net
Flávio Kannenberg	Diretor de Engenharia e SI	Coordenação técnica de controles de SI
Djiovani Douglas	Operações de TI e SI	Análise de riscos, conformidade e infraestrutura
Helton Souza	DevSecOps	Segurança no SDLC e pipeline CI/CD

** Composição vigente em 24/02/2026.*

CSG FK helt DD

Anexo II – Cronograma de Atividades Cíclicas

Atividade	Frequência	Próxima Data	Responsável
Revisão da PSI	Semestral	24/08/2026	CSI / DPO
Reunião do CSI	Trimestral	Maio/2026	CSI
Pentest externo	Semestral	Março/2026	CSI + Empresa Especializada
Varredura de vulnerabilidades	A cada 5 dias	Contínuo	TI / DevSecOps
Revisão de acessos (access review)	Trimestral	Maio/2026	TI / CSI
Treinamento de SI	Anual + admissão	Dezembro/2026	CSI
Teste de DRP/PCN	Anual	Novembro/2026	TI / DevSecOps / CSI
Backup + teste de restauração	Semestral	Agosto/2026	TI / DevOps
Auditoria interna de SI	Anual	Outubro/2026	CSI
Atualização do inventário (GLPI)	Trimestral	Maio/2026	TI

CSG FK helt DD

Anexo III – Histórico de Revisões

Versão	Data	Tipo	Responsável	Descrição
v1-v13	2020-2023	Diversas	CSI	Histórico anterior sob guarda do CSI
v14	19/02/2024	Revisão ordinária	Cleiton Garcia	Atualização de controles técnicos; assinatura (SHA-256)
v15	24/02/2026	Revisão ordinária	CSI / Cleiton Garcia	Infraestrutura AWS Ohio; Bitwarden; DevSecOps v1.1; GLPI; Logs POL-SI-LOG-001; retenção 90 dias pós-contrato; atualização CSI (Flávio Kannenberg, Djiovani Douglas, Helton Souza); cronograma 2026; LGPD formalizado.

Assinatura Eletrônica

Este documento é homologado por assinatura eletrônica com geração de hash SHA-256, conforme MP nº 2.200-2/2001 e Lei nº 14.063/2020. A versão assinada é o documento oficial e tem plena validade jurídica.

_____

Cleiton Garcia – DPO / Encarregado LGPD | dpo@upflux.net

Em nome do Comitê de Segurança da Informação (CSI) e da Diretoria Executiva

UpFlux Process Intelligence Ltda. – 24 de fevereiro de 2026

Cleiton dos Santos Garcia

Cleiton dos Santos Garcia (24 de fevereiro de 2026 14:59:57 GMT-3)

Flavio Kannenberg

Flavio Kannenberg (24 de fevereiro de 2026 15:18:01 GMT-3)

helton denis (24 de fevereiro de 2026 17:00:12 GMT-3)

Djiovani Douglas

Djiovani Douglas (24 de fevereiro de 2026 15:03:24 GMT-3)

PSI_UpFlux_v15_24022026

Relatório de auditoria final 2026-02-24

Criado em:	2026-02-24
Por:	Djiovani Douglas (djiovani@upflux.ai)
Status:	Assinado
ID da transação:	CBJCHBCAABAADeigBaSuD0fEr0UfSNrxJiIAdGB2ZlFq

Histórico de "PSI_UpFlux_v15_24022026"

Documento criado por Djiovani Douglas (djiovani@upflux.ai)
2026-02-24 - 17:57:33 GMT

Documento enviado por email para cleitonsg@upflux.ai para assinatura
2026-02-24 - 17:57:38 GMT

Documento enviado por email para flaviok@upflux.ai para assinatura
2026-02-24 - 17:57:39 GMT

Documento enviado por email para heltons@upflux.net para assinatura
2026-02-24 - 17:57:39 GMT

Documento enviado por email para Djiovani Douglas (djiovani@upflux.ai) para assinatura
2026-02-24 - 17:57:39 GMT

Email visualizado por cleitonsg@upflux.ai
2026-02-24 - 17:58:18 GMT

O signatário cleitonsg@upflux.ai inseriu o nome Cleiton dos Santos Garcia ao assinar
2026-02-24 - 17:59:55 GMT

Documento assinado eletronicamente por Cleiton dos Santos Garcia (cleitonsg@upflux.ai)
Data da assinatura: 2026-02-24 - 17:59:57 GMT - Fonte da hora: servidor

Documento assinado eletronicamente por Djiovani Douglas (djiovani@upflux.ai)
Data da assinatura: 2026-02-24 - 18:03:24 GMT - Fonte da hora: servidor

Email visualizado por flaviok@upflux.ai
2026-02-24 - 18:06:36 GMT

O signatário flaviok@upflux.ai inseriu o nome Flavio Kannenberg ao assinar
2026-02-24 - 18:17:59 GMT

Documento assinado eletronicamente por Flavio Kannenberg (flaviok@upflux.ai)

Data da assinatura: 2026-02-24 - 18:18:01 GMT - Fonte da hora: servidor

Email visualizado por heltons@upflux.net

2026-02-24 - 19:57:34 GMT

O signatário heltons@upflux.net inseriu o nome helton denis ao assinar

2026-02-24 - 20:00:10 GMT

Documento assinado eletronicamente por helton denis (heltons@upflux.net)

Data da assinatura: 2026-02-24 - 20:00:12 GMT - Fonte da hora: servidor

Contrato finalizado.

2026-02-24 - 20:00:12 GMT