UpFlux

SMART PROCESS S.A. · CNPJ 28.697.488/0001-77

Política de Segurança da Informação

Versão 16 · 27 de agosto de 2026

Código do Documento	PSI-UPFLUX-v16
Versão	16
Substitui	PSI-UPFLUX-v15 (24/02/2026)
Status	Aprovado pelo Comitê de Segurança da Informação e pela Diretoria Executiva
Data de Homologação	27/08/2026
Próxima Revisão	27/02/2027 (ciclo semestral)
Classificação	Confidencial — Distribuição Restrita
Área Proprietária	Segurança da Informação
Responsável	Carlos Eduardo Feitosa — DPO / Encarregado LGPD
E-mail DPO	dpo@upflux.net (canal institucional)
Aprovadores	Comitê de Segurança da Informação (CSI) e Diretoria Executiva

Sumário

1 Introdução

1.1 Apresentação

A **Smart Process S.A.**, sociedade empresária brasileira inscrita no CNPJ sob o nº 28.697.488/0001-77, com sede em Jaraguá do Sul, Santa Catarina, atua no mercado sob o nome fantasia **UpFlux** (doravante "UpFlux"). A empresa é especializada em Process Mining e Process Intelligence e, no segmento SaaS B2B, 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, assegurando a confidencialidade, a integridade e a disponibilidade dos dados de clientes, colaboradores e parceiros, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais normas aplicáveis.

> **Referenciais normativos adotados.** A ABNT NBR ISO/IEC 27001:2022 e o NIST Cybersecurity Framework são adotados como referenciais de controles e de gestão de riscos. A adoção desses referenciais orienta o desenho e a operação dos controles descritos nesta política e **não constitui declaração de certificação** por organismo acreditado.

1.2 Objetivos

- Proteger os ativos de informação da UpFlux contra ameaças internas e externas;
- Assegurar conformidade com a LGPD (Lei nº 13.709/2018), com as regulamentações da ANPD e com as regulamentações da ANS aplicáveis a contextos de saúde;
- Garantir a continuidade dos negócios e a resiliência operacional;
- Estabelecer padrões de conduta para colaboradores, terceiros e prestadores de serviços;
- Manter os controles de segurança alinhados aos referenciais ABNT NBR ISO/IEC 27001:2022 e NIST Cybersecurity Framework;
- Assegurar consistência entre o que esta política declara e o que a operação executa, mediante revisão periódica e reconciliação com as políticas satélites.

1.3 Declaração da Administração

A Diretoria Executiva da UpFlux declara seu comprometimento com a segurança da informação, destinando recursos humanos, financeiros e tecnológicos para a implementação e a 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.

O comprometimento da Alta Direção é formalizado pela aprovação desta política, registrada no Anexo III e evidenciada pela assinatura eletrônica constante ao final deste documento.

1.4 Escopo

Esta política se aplica a:

- Todos os colaboradores da UpFlux (CLT, PJ e estagiários);

- 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 de forma **exclusiva** na Amazon Web Services (AWS), região **us-east-2 (Ohio, Estados Unidos)**;
- Ambiente local (on-premises) da sede administrativa em Jaraguá do Sul/SC, protegido pelo firewall Fortinet FortiGate 60F.

1.5 Conceitos e Definições

Termo	Definição
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.
Evento de Segurança	Ocorrência identificada em sistema, serviço ou rede que indique possível falha de controle, sem comprometimento confirmado.
Incidente de Segurança	Evento ou conjunto de eventos que comprometa ou ameace a confidencialidade, a integridade ou a disponibilidade da informação.
Incidente de Privacidade	Incidente de segurança que envolva dados pessoais.
PAM	Privileged Access Management. Conjunto de controles para gestão e auditoria de acessos privilegiados.

1.6 Documentos Relacionados

Esta política é o documento normativo de topo do Sistema de Gestão de Segurança da Informação da UpFlux e deve ser lida em conjunto com:

Documento	Código / Versão
Política de Classificação e Manuseio da Informação	PCI-SEC-001 v1.1
Política de Gestão de Acessos	POL-SI-ACESSO-001 v1.0
Política de Senhas e Autenticação	PSA v1.2
Procedimento de Revisão de Acesso (Access Review)	—
Política de Offboarding e Revogação de Acessos	—
Política de Controle de Acesso em Nuvem	CAC-SEC-001 v1.0
Política de Gestão de Ativos	PSI-ATV-001 v1.1
Política de Desenvolvimento Seguro (DevSecOps)	PS-SEC-DEVSECOPS v1.1
Processo de Gestão de Vulnerabilidades	POL-SI-VULN-001 v1.0
Política de Gestão de Patches e Atualizações de Segurança	PS-SEC-PATCH v1.1
Política de Gestão de Incidentes de Segurança da Informação	PSI-INC-001 v1.0
Política de Retenção, Imutabilidade e Disponibilização de Logs	POL-SI-LOG-001 v1.1
Política de Segurança de Servidores	—
Política de Privacidade (Privacy by Design / Privacy by Default)	—
Política de Coleta Mínima de Dados e Consentimento Informado	—
Política de Anonimização e Pseudonimização de Dados	—
Política de Relatório de Impacto à Proteção de Dados (RIPD/DPIA)	—
Política e Procedimento de Devolução e Descarte de Dados ao Término do Contrato	v1.1
Procedimento Operacional Padrão de Descarte de Dados	POP-DESC-001
Plano de Continuidade de Negócios / Plano de Recuperação de Desastres	PCN / DRP
Plano de Governança de Gestão de Riscos	POL-SI-RISCO-001
Política de Governança de IA Generativa (GenAI/LLM) e de Machine Learning	PS-GOV-GENAI-001 / PS-GOV-ML-001
Política de Homologação e Controle de Software	—
Política de Conscientização e Treinamento em SI e Privacidade	—

Documento	Código / Versão
Cláusulas Contratuais Padrão de Privacidade e Proteção de Dados	—

1.7 Autoria

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

1.8 Divulgação e Distribuição

Esta política é de ciência obrigatória para todos os colaboradores e está disponível no repositório corporativo de políticas. Versão resumida pode ser disponibilizada a clientes e parceiros mediante solicitação formal. A distribuição do documento completo a terceiros depende de autorização do CSI e de instrumento de confidencialidade vigente.

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 de modelo de negócio; alteração regulatória (LGPD, ANS, ANPD); ou alteração na composição do CSI. A próxima revisão programática está agendada para **27/02/2027**.

A cada revisão desta política, as políticas satélites que a referenciam devem ter suas citações de versão atualizadas, de modo a evitar remissão a versão revogada.

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, deliberar sobre exceções e aceites de risco e coordenar a resposta a incidentes. A composição vigente consta no Anexo I. As reuniões ordinárias são trimestrais e as extraordinárias são convocadas em caso de incidente relevante.

1.10.2 Inventário de Ativos

A UpFlux mantém inventário formal e atualizado de todos os ativos de informação por meio da ferramenta **Tactical RMM**, complementado pelos inventários nativos dos provedores de nuvem para ativos em AWS. O inventário abrange estações de trabalho, servidores, equipamentos de rede, software licenciado, ativos em nuvem e documentos críticos. Cada ativo possui Dono de Ativo (Asset Owner) formalmente designado, responsável pela classificação e proteção adequadas, conforme a PCI-SEC-001 e a PSI-ATV-001. 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 e no Plano de Governança de Gestão de Riscos (POL-SI-RISCO-001), 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 a LGPD (Lei nº 13.709/2018), sob a responsabilidade do Encarregado Carlos Eduardo Feitosa (dpo@upflux.net), e com as regulamentações da ANS aplicáveis em contextos de saúde. A ABNT NBR ISO/IEC 27001:2022 e o NIST Cybersecurity Framework são utilizados como referenciais de controles e de gestão, conforme a seção 1.1.

1.10.5 Treinamento e Conscientização

Todos os colaboradores passam por treinamento de segurança da informação e privacidade na admissão e anualmente, conforme a Política de Conscientização e Treinamento. Campanhas adicionais, incluindo simulações de phishing, são realizadas após incidentes relevantes ou atualizações desta política.

2 Segurança Cibernética

2.1 Autenticação e Controle de Acesso

2.1.1 Política Geral de Acesso

- O acesso a sistemas e dados da UpFlux é concedido com base no princípio do menor privilégio (least privilege) e na necessidade de conhecer (need-to-know);
- As contas de acesso são individuais e intransferíveis. É vedado o uso de credenciais compartilhadas;
- O provisionamento de acessos é formalizado pelo gestor responsável e executado pela área de TI, com segregação entre quem solicita, quem aprova e quem executa, conforme POL-SI-ACESSO-001;
- As revisões de acessos (access review) para usuários padrão e privilegiados são realizadas **trimestralmente**, com registro formal para fins de auditoria. Esta política é a fonte normativa da periodicidade referenciada pelas políticas satélites;
- No desligamento de colaboradores, todos os acessos são revogados em **até 24 horas** após a comunicação formal do RH, com desativação de contas e credenciais, conforme a Política de Offboarding e Revogação de Acessos;
- Na transferência ou no desligamento de colaborador com acesso a credenciais institucionais, tais credenciais são obrigatoriamente alteradas, conforme a seção 3.7.2.

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 corporativa, console AWS, plataforma de banco de dados, ferramentas DevOps e painéis administrativos. A autenticação é centralizada no **Microsoft Entra ID** (OIDC), com aplicação de políticas de acesso condicional conforme perfil e risco de acesso. A exigência de segundo fator é imposta automaticamente a partir do primeiro acesso do colaborador.

2.1.3 Gestão de Credenciais Privilegiadas (PAM)

- **Cofre de senhas corporativo (Bitwarden):** todas as senhas institucionais e segredos de serviço são gerenciados no Bitwarden, ferramenta homologada pelo CSI, com acesso controlado por MFA e auditado;
- **Identidades gerenciadas na AWS:** os 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 nem acesso SSH habilitado. Todas as interações administrativas ocorrem via console do provedor, APIs, pipelines CI/CD ou Infraestrutura como Código;
- **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

- Todos os endpoints corporativos possuem solução EDR implantada: **Bitdefender GravityZone**, com cobertura de 100% dos dispositivos gerenciados;

- Em razão do modelo de trabalho predominantemente remoto, o EDR constitui a camada primária de proteção da frota, independentemente da existência de perímetro de rede corporativa;
- Atualização de assinaturas automática, com janela máxima de 24 horas;
- Varreduras agendadas a cada 5 dias em todos os endpoints;
- Feeds de Threat Intelligence integrados ao GravityZone e ao SIEM Elastic Security, para detecção baseada em indicadores de comprometimento atualizados;
- Alertas de detecção encaminhados automaticamente ao time de Segurança da Informação via integração com o Elastic Security;
- A gestão de dispositivos corporativos é apoiada pelo Microsoft Intune;
- **Dispositivos não gerenciados (BYOD)** não são autorizados a acessar sistemas corporativos. Quando excepcionalmente autorizados, dependem de aprovação formal do CSI e passam a ser tratados como ativos de informação, sujeitos aos requisitos mínimos de segurança e à possibilidade de revogação remota e limpeza seletiva de dados corporativos, conforme a PSI-ATV-001.

2.3 Firewall e Proteção de Perímetro

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

2.4 Testes de Intrusão (Pentest)

- Pentest externo e interno com periodicidade **semestral**, executado por empresa especializada independente, com um ciclo no primeiro e outro no segundo semestre de cada exercício. As datas de execução de cada ciclo constam no Anexo II;
- Após cada pentest, um Plano de Ação com prazos e responsáveis é formalizado pelo CSI e acompanhado até o encerramento;
- Os achados são tratados conforme os prazos de remediação da seção 2.5, sendo os de severidade crítica remediados em **até 2 dias úteis**;
- Achados que caracterizem comprometimento de confidencialidade, integridade ou disponibilidade são classificados formalmente contra os critérios de materialidade da PSI-INC-001, com registro da decisão;
- Os relatórios técnicos são classificados como Restritos. A clientes é disponibilizado Resumo Executivo de Teste de Intrusão, e o relatório integral somente mediante instrumento de confidencialidade e aprovação do CSI.

2.5 Gestão de Vulnerabilidades e Atualizações

- Varredura automática de vulnerabilidades a cada 5 dias em toda a infraestrutura (endpoints, servidores, containers e ambiente AWS);
- Análise de composição de software (SCA) integrada ao pipeline CI/CD, para detecção de dependências com CVEs conhecidos;

- Imagens de container reconstruídas periodicamente para incorporar correções de segurança;
- Aplicação de patches de forma gradual e controlada, com separação por ambientes (desenvolvimento, homologação e produção) e validação prévia à promoção, conforme PS-SEC-PATCH.

Os prazos de remediação são priorizados pela pontuação CVSS e são únicos para toda a documentação da UpFlux:

Severidade	Faixa CVSS	Prazo de remediação
Crítica	9,0 a 10,0	2 dias úteis
Alta	7,0 a 8,9	14 dias
Média	4,0 a 6,9	30 dias
Baixa	0,1 a 3,9	Conforme planejamento ou próximo ciclo

Exceções a estes prazos exigem justificativa formal, controles compensatórios e aceite de risco aprovado pelo CSI.

2.6 Criptografia e Gestão de Chaves

- **Dados em repouso:** AES-256 em todos os ambientes, incluindo MongoDB Atlas, Amazon S3 e volumes EBS;
- **Dados em trânsito:** TLS 1.2 ou superior em todas as comunicações, com HTTPS forçado (HSTS) nas aplicações web;
- **Gestão de chaves:** AWS KMS com rotação automática e controle de uso via IAM. A eliminação definitiva de dados de cliente é apoiada por crypto-shredding por tenant;
- **Segredos e credenciais:** gerenciados no Bitwarden e/ou no AWS Secrets Manager, com rotação periódica. É vedado o armazenamento em código-fonte ou em arquivos de configuração em texto claro;
- **Algoritmos obsoletos** (MD5, SHA-1, DES, SSL 3.0, TLS 1.0 e TLS 1.1) são expressamente vedados.

2.7 Proteção contra Vazamento de Dados

A UpFlux **não utiliza ferramenta dedicada de Data Loss Prevention (DLP)**. A proteção contra vazamento de informações é sustentada pelo conjunto de controles abaixo, aplicados de forma combinada:

- Classificação e rotulagem obrigatórias da informação nos níveis Pública, Interna, Confidencial e Restrita, conforme PCI-SEC-001, com requisitos mínimos de proteção definidos por nível;
- Controle de dispositivos e de mídias removíveis nos endpoints, aplicado por política no Bitdefender GravityZone;
- Filtragem de conteúdo e inspeção de tráfego no perímetro da sede, via Fortinet FortiGate 60F;
- Vedação ao armazenamento de informações Confidenciais e Restritas em dispositivos pessoais, mídias não gerenciadas ou serviços de nuvem não homologados;
- Vedação ao envio de dados de clientes por canais não corporativos ou não criptografados;

- Monitoramento e retenção de trilhas de acesso a dados de clientes via AWS CloudTrail e Elastic Security, permitindo detecção e investigação a posteriori.

> A implantação de ferramenta dedicada de DLP está registrada no Plano de Tratamento de Riscos como controle a avaliar, não constituindo controle vigente. Respostas a questionários de clientes devem refletir esta seção.

2.8 Rastreabilidade e Monitoramento

2.8.1 SIEM e Monitoramento em Nuvem

- **Elastic Security (SIEM):** centralização, correlação e análise de logs de aplicação e de infraestrutura, integrado a AWS CloudTrail, GuardDuty e CloudWatch;
- **AWS CloudTrail:** auditoria de todas as ações na conta AWS, incluindo chamadas de API, acesso ao console e alterações de configuração;
- **AWS GuardDuty:** detecção de ameaças e de comportamentos anômalos na infraestrutura em nuvem;
- **Amazon CloudWatch:** monitoramento de métricas operacionais e alertas de desempenho;
- **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 a POL-SI-LOG-001, com retenção mínima operacional de 90 dias no repositório central, exportação controlada antes de qualquer expurgo, proteção WORM contra alteração indevida para logs de segurança, acesso e auditoria, e disponibilização para auditorias e investigações mediante processo formal com segregação de funções.

2.8.3 Threat Intelligence

Feeds de inteligência de ameaças são integrados ao Elastic Security e ao Bitdefender GravityZone, permitindo detecção baseada em indicadores de comprometimento continuamente atualizados.

3 Segurança Lógica

3.1 Acesso à Internet

- O acesso à internet em dispositivos corporativos está sujeito a monitoramento e filtragem de conteúdo, aplicados no endpoint e, quando o dispositivo estiver na sede, também no perímetro;
- O download ou a execução de softwares não homologados pela área de TI é expressamente proibido, conforme a Política de Homologação e Controle de Software.

3.2 Acesso Remoto e Rede Corporativa

A UpFlux opera com força de trabalho predominantemente remota. O modelo de acesso é baseado em identidade e em postura do dispositivo, não em perímetro de rede.

- O acesso a sistemas e aplicações corporativas ocorre por meio de identidade federada no **Microsoft Entra ID**, com MFA obrigatório e aplicação de políticas de acesso condicional, independentemente da localização do usuário;
- A **VPN corporativa (Fortinet FortiClient)** é utilizada para acesso a recursos internos do ambiente local da sede, condicionada a autenticação forte e menor privilégio. A VPN **não constitui requisito** para acesso às aplicações hospedadas em nuvem;
- Dispositivos sem o agente EDR instalado e atualizado não são autorizados a acessar recursos corporativos;
- As sessões são protegidas por expiração automática por inatividade e bloqueio de tela, com políticas aplicadas centralmente no Entra ID.

3.3 Armazenamento e Manuseio de Informações

3.3.1 Classificação da Informação

Toda informação deve ser classificada conforme a PCI-SEC-001 nos níveis Pública, Interna, Confidencial e Restrita. Informações que contenham dados pessoais são classificadas no mínimo como Confidenciais e, quando envolverem dados pessoais sensíveis, como Restritas.

3.3.2 Armazenamento Autorizado

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

3.3.3 Transmissão

Toda transmissão de informações Confidenciais e Restritas deve utilizar canais criptografados (TLS 1.2 ou superior). É vedado o envio por e-mail pessoal ou por 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, Estados Unidos), utilizada de forma exclusiva. Componentes principais:

Componente	Tecnologia e controles
Banco de dados	MongoDB Atlas (us-east-2), banco dedicado por cliente em cluster de no mínimo três nós, com AES-256 em repouso e TLS 1.2+ em trânsito
Armazenamento de objetos	Amazon S3 com criptografia SSE-S3 / SSE-KMS
Processamento	Containers orquestrados e promovidos via pipeline CI/CD
Gestão de chaves	AWS KMS com rotação automática
Monitoramento	AWS CloudTrail, GuardDuty, CloudWatch e Elastic Security (SIEM)

> **Transferência internacional de dados.** O tratamento de dados em região fora do território nacional caracteriza transferência internacional para os fins do art. 33 da LGPD. A UpFlux declara essa condição de forma consistente em todos os questionários, contratos e registros de tratamento, sustentada por cláusulas contratuais de proteção de dados, controles técnicos de criptografia e segregação por tenant.

3.3.5 Backup e Recuperação

Política de backup em três camadas de retenção, com todos os backups criptografados e armazenados de forma segregada do ambiente principal:

Camada	Frequência	Retenção
Incremental	A cada 6 horas	Conforme ciclo de sobrescrita
Semanal	Semanal	30 dias
Mensal	Mensal	6 meses

Os testes de restauração são executados com periodicidade **semestral**, no mínimo, com registro formal do resultado, e adicionalmente após mudanças relevantes de arquitetura. Backups que contenham dados de clientes são classificados como Restritos.

Objetivos de recuperação (conforme DRP): RPO de até 4 horas e RTO de até 8 horas. Tais valores constituem **objetivos de recuperação de desastre** e não indicadores de nível de serviço sujeitos a penalidade contratual, salvo quando expressamente previsto em instrumento contratual específico.

3.3.6 Retenção e Descarte de Dados de Clientes

Após o encerramento do contrato, os dados do cliente são mantidos por até **90 (noventa) dias**, conforme os instrumentos contratuais aplicáveis, prazo no qual o cliente pode solicitar a exportação de seus dados. Encerrado o prazo, os dados são definitivamente eliminados de todos os ambientes, conforme a Política e Procedimento de Devolução e Descarte de Dados ao Término do Contrato e o POP-DESC-001, abrangendo banco de dados dedicado, estruturas OLAP, cluster principal, identidades associadas e dados brutos de ingestão.

Cada execução gera registro formal rastreável e certificado de destruição enviado ao cliente, com atualização do Registro de Atividades de Tratamento. O descarte é irreversível e impede a recuperação das informações.

3.4 Propriedade Intelectual

- Código-fonte, documentação e desenvolvimentos realizados na UpFlux são de propriedade exclusiva da empresa;
- É vedada a reprodução de softwares sem licença válida;
- O uso de bibliotecas open source deve ser avaliado quanto à compatibilidade de licença e à existência de vulnerabilidades, via processo SCA no pipeline de desenvolvimento.

3.5 Uso de Sistemas Corporativos

- Os sistemas corporativos destinam-se exclusivamente a finalidades profissionais;
- Toda instalação de software em dispositivos corporativos requer aprovação da área de TI;
- O acesso a sistemas de clientes é limitado ao mínimo necessário, registrado, justificado e sujeito a autorização prévia do cliente quando envolver seu ambiente.

3.6 Uso de E-mails

- O e-mail corporativo destina-se exclusivamente a comunicações profissionais;
- Informações Confidenciais e Restritas devem ser enviadas por canais criptografados ou plataformas autorizadas;
- É vedado o encaminhamento de e-mails corporativos para contas pessoais;
- O acesso a e-mail pessoal em dispositivos corporativos durante o expediente não é permitido.

3.7 Uso de Senhas

3.7.1 Diretrizes gerais

Os requisitos de senha desta seção são idênticos aos da Política de Senhas e Autenticação (PSA v1.2), que é o documento de detalhe do tema.

- A senha é pessoal e intransferível, sendo o colaborador responsável pelas ações realizadas com suas credenciais;
- Senhas não devem ser compartilhadas sob nenhuma circunstância;
- **Comprimento mínimo de 8 caracteres, com ao menos 3 das 4 categorias:** letras maiúsculas, letras minúsculas, números e caracteres especiais;
- É proibido o reuso das últimas 3 versões de senha;
- A alteração de senha é obrigatória e imediata em caso de suspeita de comprometimento;
- **O armazenamento no cofre corporativo Bitwarden é obrigatório.** É vedado o registro de senhas em arquivos não criptografados ou em meio físico;
- Bloqueio temporário da conta após 5 tentativas de acesso inválidas consecutivas;
- Senhas temporárias devem ser substituídas no primeiro acesso;
- As senhas de usuários da plataforma são armazenadas de forma irreversível (hash), e as mensagens de erro de autenticação são genéricas.

3.7.2 Senhas institucionais

- Todas as senhas institucionais possuem responsável formalmente definido e são armazenadas no Bitwarden corporativo;
- As senhas institucionais são obrigatoriamente alteradas sempre que colaborador com acesso for transferido ou desligado, com registro da execução;
- Segredos de integração e de contas de serviço seguem processo de rotação periódica.

3.8 Mensageria Corporativa

- Somente o **Microsoft Teams** é homologado para comunicações corporativas internas;
- Aplicações pessoais de mensageria não devem ser utilizadas para comunicações que envolvam informações Confidenciais ou Restritas. Esta vedação aplica-se à comunicação corporativa e não se confunde com os canais de notificação configuráveis do produto.

3.9 Gerenciamento de Partes Externas

- Prestadores de serviço devem assinar termo de confidencialidade antes de receber qualquer acesso;
- O acesso de terceiros é provisionado com menor privilégio, prazo definido e monitoramento;
- Os contratos devem incluir cláusulas de segurança e de proteção de dados conforme as Cláusulas Contratuais Padrão de Privacidade.

3.10 Segurança Física

- O acesso físico às instalações da sede administrativa é controlado e monitorado;
- Equipamentos corporativos não devem ser deixados sem supervisão em locais públicos;
- O bloqueio automático de tela é ativo e obrigatório em todos os dispositivos;
- A infraestrutura de produção é operada em data centers do provedor de nuvem, cujos controles físicos e ambientais são de responsabilidade do provedor e evidenciados por seus relatórios de conformidade públicos.

3.11 Controle de Equipamentos

- Todo equipamento corporativo é registrado no inventário corporativo (**Tactical RMM**) antes de ser colocado em uso;
- Movimentação, substituição ou descarte devem ser comunicados à área de TI para atualização do inventário e execução de descarte seguro, com eliminação verificável dos dados.

3.12 Controle de Documentos Físicos

- Documentos físicos Confidenciais e Restritos devem ser armazenados em local trancado;
- O descarte deve ser realizado por fragmentadora de papel ou serviço de descarte seguro certificado.

4 Políticas de Processos Internos

4.1 Desenvolvimento Seguro (DevSecOps)

A UpFlux adota abordagem DevSecOps, integrando segurança em todas as fases do ciclo de vida de desenvolvimento, conforme a PS-SEC-DEVSECOPS. Controles mínimos por fase:

Fase	Controle mínimo
Planejamento	Modelagem de ameaças (Threat Modeling)
Desenvolvimento	Plugins de segurança na IDE, com alerta de código inseguro em tempo real
Build / CI	Análise estática (SAST) e análise de composição de software (SCA)
Testes	Análise dinâmica (DAST) em ambiente de homologação
Deploy / CD	Validação de IaC com auditoria de configurações
Operação	Monitoramento contínuo via Elastic Security e logs auditados

Todas as mudanças em produção passam por fluxo controlado de revisão e aprovação no pipeline CI/CD, com rastreabilidade completa e segregação entre quem desenvolve e quem aprova a promoção.

4.2 Gestão de Incidentes de Segurança

A UpFlux mantém processo formal de gestão de incidentes conforme a PSI-INC-001. Os incidentes são registrados em ferramenta de gestão e classificados por impacto nos níveis Baixo, Médio, Alto e Crítico. Incidentes classificados como Médio, Alto ou Crítico exigem envolvimento imediato da Segurança da Informação para contenção, erradicação e recuperação.

A distinção entre **evento de segurança** e **incidente de segurança** é formalmente registrada contra os critérios de materialidade da PSI-INC-001, com fundamentação da decisão mantida como evidência.

Incidentes com possível impacto a dados pessoais são comunicados ao DPO, que avalia o risco aos titulares e a necessidade de comunicação. Quando devida, a comunicação à ANPD e aos titulares é realizada em **até 3 (três) dias úteis** contados do conhecimento do incidente, conforme o art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024. Clientes contratantes afetados são notificados conforme os prazos previstos nos respectivos instrumentos contratuais.

4.3 Continuidade de Negócios e Recuperação de Desastres

A UpFlux mantém Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP) ativos, testados no mínimo anualmente e após mudanças relevantes de ambiente, com resultados documentados. Objetivos de recuperação: RPO de até 4 horas e RTO de até 8 horas, nos termos da seção 3.3.5.

4.4 Gestão de Fornecedores e Terceiros

A contratação de fornecedores que acessarão dados ou sistemas exige avaliação de segurança prévia (due diligence), assinatura de termo de confidencialidade e de acordo de tratamento de dados quando aplicável, cláusulas de segurança no contrato e monitoramento do acesso concedido. Fornecedores que

atuem como operadores de dados pessoais estão sujeitos às obrigações da LGPD. Os suboperadores relevantes da cadeia de tratamento são declarados aos clientes no Registro de Atividades de Tratamento.

4.5 Privacidade e Proteção de Dados (LGPD)

A UpFlux adota Privacy by Design e Privacy by Default em seus produtos e processos. O Encarregado pelo Tratamento de Dados Pessoais é **Carlos Eduardo Feitosa**, cujo canal institucional de contato é **dpo@upflux.net**. A designação vigente tem efeito desde 23/06/2026, formalizada em ata de transição específica. A identidade e o contato do Encarregado são divulgados publicamente no sítio eletrônico da UpFlux, conforme o art. 41, §1º, da LGPD. O canal institucional dpo@upflux.net é mantido independentemente do titular da função, de modo a preservar a continuidade do atendimento a titulares e à autoridade em caso de sucessão. O tratamento de dados pessoais ocorre com base legal definida, finalidade específica e minimização, e o Registro de Atividades de Tratamento (RAT/ROPA) é mantido atualizado pelo DPO.

Os dados tratados na plataforma são aqueles disponibilizados pelo cliente no processo de ingestão, podendo ser anonimizados na origem conforme definição contratual. Quando o tratamento envolver dados pessoais sensíveis, inclusive dados de saúde, aplica-se avaliação de necessidade de Relatório de Impacto à Proteção de Dados (RIPD/DPIA), conforme política específica.

4.6 Auditoria e Conformidade

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

As evidências de conformidade próprias da UpFlux consistem em suas políticas homologadas, registros operacionais e relatórios de teste de intrusão. Relatórios de conformidade de provedores de nuvem, quando obtidos sob confidencialidade, não são repassados a terceiros, sendo indicadas as versões públicas equivalentes.

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 a regularização;
- Medidas disciplinares administrativas, incluindo demissão por justa causa;
- Rescisão contratual imediata para prestadores de serviço;
- Responsabilização civil e criminal nos termos da legislação brasileira aplicável, incluindo a LGPD.

A aplicação de medidas disciplinares é de responsabilidade do CSI em conjunto com a Diretoria Executiva e, quando aplicável, com o setor jurídico. A UpFlux reserva-se o direito de acionar as autoridades competentes diante de evidências de crimes cibernéticos ou de violações à LGPD.

Anexo I — Comitê de Segurança da Informação (CSI)

Reuniões ordinárias trimestrais. Reuniões extraordinárias convocadas em caso de incidente relevante.

Membro	Cargo / Função	Responsabilidade no CSI
Carlos Eduardo Feitosa	DPO / Encarregado LGPD	Presidência do CSI, conformidade LGPD e privacidade (dpo@upflux.net)
Cleiton Garcia	Diretor de Produto e IA	Representação da Diretoria Executiva, aprovação de políticas e de aceites de risco
Djiovani Douglas	Coordenador de TI e Segurança da Informação	Gestão de riscos, conformidade, infraestrutura e coordenação dos controles de SI
Helton Souza	Líder de Engenharia de Operações e DevSecOps	Coordenação técnica dos controles de SI, segurança no SDLC e no pipeline CI/CD

Composição vigente em 27/08/2026. A presidência do CSI é exercida pelo Encarregado, de modo a preservar a independência da função na avaliação de riscos de privacidade.

Anexo II — Cronograma de Atividades Cíclicas

Este anexo estabelece a periodicidade obrigatória e a janela de execução de cada atividade cíclica. As datas efetivas de execução de cada ciclo são registradas na ata de reunião do CSI e nos registros operacionais correspondentes, que constituem a evidência de cumprimento.

Atividade	Periodicidade	Janela de execução	Responsável
Revisão desta política	Semestral	Fevereiro e agosto	CSI / DPO
Reunião ordinária do CSI	Trimestral	Um ciclo por trimestre	CSI
Pentest externo e interno	Semestral	Um ciclo por semestre	CSI e empresa especializada
Varredura de vulnerabilidades	A cada 5 dias	Contínua e automatizada	TI / Engenharia de Operações
Revisão de acessos (access review)	Trimestral	Um ciclo por trimestre	TI / CSI
Treinamento de SI e privacidade	Anual e na admissão	Segundo semestre	CSI
Teste de DRP e PCN	Anual	Segundo semestre	TI / Engenharia de Operações / CSI
Teste de restauração de backup	Semestral	Um ciclo por semestre	TI / Engenharia de Operações
Auditoria interna de SI	Anual	Segundo semestre	CSI
Atualização do inventário de ativos	Trimestral	Um ciclo por trimestre	TI
Revisão do Plano de Tratamento de Riscos	Semestral	Fevereiro e agosto	CSI

O descumprimento de janela de execução é registrado como não conformidade e tratado com plano de ação aprovado pelo CSI.

Anexo III — Histórico de Revisões

Versão	Data	Responsável	Descrição
v1 a v13	2020 a 2023	CSI	Histórico anterior sob guarda do CSI
v14	19/02/2024	Cleiton Garcia	Atualização de controles técnicos e adoção de assinatura eletrônica com hash SHA-256
v15	24/02/2026	CSI / Cleiton Garcia	Infraestrutura AWS Ohio; Bitwarden; DevSecOps v1.1; inventário; POL-SI-LOG-001; retenção de 90 dias pós-contrato; atualização da composição do CSI; cronograma 2026; formalização LGPD
v16	27/08/2026	CSI / Segurança da Informação	Revisão ordinária semestral com reconciliação documental. Correção da razão social para Smart Process S.A. (nome fantasia UpFlux) com inclusão de CNPJ; ISO/IEC 27001:2022 e NIST CSF reposicionados como referenciais adotados, com declaração expressa de ausência de certificação; remoção de menção a reconhecimento de mercado por não constituir controle de segurança; inventário de ativos corrigido de GLPI para Tactical RMM (seções 1.10.2, 3.11 e Anexo II); banco de dados de produção corrigido de Amazon RDS para MongoDB Atlas (seções 2.6 e 3.3.4); acesso remoto reescrito para refletir o modelo baseado em identidade, com VPN restrita a recursos internos da sede (seção 3.2); seção 2.7 reescrita, com declaração expressa de ausência de ferramenta dedicada de DLP e descrição dos controles efetivamente vigentes; unificação do prazo de remediação de vulnerabilidade crítica em 2 dias úteis (seções 2.4 e 2.5); remoção dos meses fixos do ciclo de pentest; inclusão da periodicidade semestral de teste de restauração e reposicionamento de RPO e RTO como objetivos de recuperação; requisitos de senha alinhados à PSA v1.2 (8 caracteres e 3 de 4 categorias), mantida a obrigatoriedade do cofre corporativo; reconciliação do tratamento de BYOD com a PSI-ATV-001; inclusão do prazo de 3 dias úteis para comunicação à ANPD conforme Resolução CD/ANPD nº 15/2024; substituição da referência contratual incorreta na retenção pós-contrato; inclusão de declaração expressa de transferência internacional de dados (art. 33, LGPD); atualização da lista de documentos relacionados com códigos e versões vigentes; distinção formal entre evento e incidente de segurança; atualização da composição do CSI, com saída de Flávio Kannenberg e assunção das atribuições técnicas por Helton Souza, registro da designação de Carlos Eduardo Feitosa como Encarregado pelo Tratamento de Dados Pessoais, com efeito desde 23/06/2026, em substituição a Cleiton Garcia, e assunção da cadeira de representação da Diretoria Executiva por Cleiton Garcia na qualidade de Diretor de Produto e IA; adoção de dpo@upflux.net como canal institucional do Encarregado, independente de titular; inclusão da obrigação de divulgação pública da identidade e do contato do Encarregado nos termos do art. 41, §1º, da LGPD; reformulação do Anexo II, que passa a declarar periodicidade e janela de execução em lugar de datas fixas, eliminando o vencimento do cronograma entre revisões

Homologação

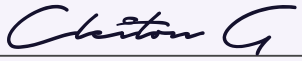
Este documento é homologado por assinatura eletrônica com geração de hash SHA-256, conforme a MP nº 2.200-2/2001 e a Lei nº 14.063/2020. A versão assinada é o documento oficial e tem plena validade jurídica.

Smart Process S.A. (UpFlux) — Jaraguá do Sul/SC, 27 de agosto de 2026.

Carlos Eduardo Feitosa
DPO / Encarregado LGPD · Presidente do CSI

Djiovani Douglas
Coordenador de TI e Segurança da Informação

Helton Souza
Líder de Engenharia de Operações e DevSecOps



Cleiton dos Santos Garcia
Diretor de Produto e IA · Diretoria Executiva