Declaração da Liderança: A alta direção da Surfix Cloud & Data Center declara que segurança da informação e privacidade são pilares estratégicos do negócio. A organização compromete-se a implementar, manter e melhorar continuamente seu sistema de gestão de segurança da informação, privacidade e privacidade em nuvem.

Apresentação: Este documento consolida as diretrizes de segurança da informação, privacidade e segurança em nuvem da Surfix em um único instrumento.

Objetivo: Garantir confidencialidade, integridade, disponibilidade e privacidade das informações, assegurando conformidade legal, continuidade do negócio, prevenção de incidentes e promoção de uma cultura organizacional de segurança e privacidade.

Referências Normativas: LGPD (Lei 13.709/2018) · Marco Civil da Internet (Lei 12.965/2014) · Lei de Crimes Cibernéticos (Lei 12.737/2012) · ISO/IEC 27001 · ISO/IEC 27701 · ISO/IEC 27017 · ISO/IEC 27018.

Diretrizes Gerais de Segurança da Informação: A Surfix estabelece políticas e controles para proteger informações contra ameaças internas e externas, gerir riscos, assegurar continuidade do negócio, tratar incidentes de forma estruturada e promover conscientização contínua. As obrigações específicas em ambientes de nuvem estão detalhadas na seção "Proteção de Dados Pessoais em Nuvem.

Comitê gestor atual:

Cargo	Responsável
Encarregada (DPO)	Patrícia Fracassio — lgpd@surfix.com.br | (81) 3419-8525 Designada como canal oficial de privacidade e proteção de dados da organização.
Cargo	**Responsável**
Analista de Qualidade	Colaboradora designada para atender junto a área de qualidade.
BDM de produtos	Colaborador designado para atender junto à área de Produtos.
Diretor de Produtos e Inovação	Diretor designado junto ao DPO para aprovar e garantir a conformidade.
Head de Cibersegurança	Profissional designado para atender junto à área de Cibersegurança.

Nomeação formal do Comitê Gestor de Segurança da Informação e Privacidade (CGSIP): Para fins de governança do SGSIP, o comitê gestor está formalmente organizado por área: Diretoria (DPO e Diretor de Produtos e Inovação), Qualidade (Analista de Qualidade), Produtos (BDM de Produtos) e Cibersegurança (Head de Cibersegurança).

Escopo e aplicação - Esta política se aplica a toda a organização e a quem se relaciona com ela:

Público	Esta política se aplica quando.
Colaboradores e estagiários	Desde o início do processo seletivo e até 20 anos após rescisão contratual, conforme critérios de retenção documentados pela área de Gente e Gestão.
Candidatos a vagas	Durante o processo seletivo e por até 18 meses após, caso não haja contratação imediata.
Parceiros e terceiros autorizados	Sempre que tiverem acesso a dados pessoais tratados pela Surfix.
Fornecedores e prestadores	No processo de contratação, durante a prestação do serviço e até 5 anos após rescisão.

Público	Esta política se aplica quando.
Clientes e usuários	Em todo o ciclo comercial: proposta, contrato, suporte e até 5 anos após rescisão.
Serviços Cloud Server (nuvem pública)	Quando a Surfix atuar como Operadora de Dados Pessoais (PII Processor) no ambiente multi-tenant.

Papéis e responsabilidades:

Quem	O que deve fazer
Alta Gestão	Aprovar políticas, prover recursos, definir apetite ao risco e patrocinar a cultura de privacidade na organização.
Encarregado (DPO)	Ser o canal com titulares e a ANPD; orientar as áreas; assegurar governança de privacidade.
Comitê Gestor	Mapear e atualizar o ROPA; avaliar riscos, contratos e provedores de nuvem; implementar controles; apoiar em incidentes; monitorar conformidade; manter registros e relatórios.
Gestores de área	Garantir que suas equipes sigam os procedimentos; participar do mapeamento de tratamentos.
Colaboradores	Cumprir esta política, participar de treinamentos obrigatórios e se houver, reportar incidentes imediatamente.
Fornecedores e prestadores	Tratar dados conforme esta política e contratos firmados; notificar a Surfix em caso de incidente. Não subcontratar o tratamento de dados pessoais sem autorização prévia e por escrito da Surfix. A Surfix manterá lista de suboperadores autorizados disponível ao Controlador de acordo com esta política.

Definições essenciais - Para facilitar a leitura deste documento, veja abaixo o significado dos principais termos utilizados:

Termo	O que significa na prática
Dado pessoal	Qualquer informação que identifica ou pode identificar uma pessoa (ex.: nome, CPF, e-mail, telefone).
Dado sensível	Dados sobre saúde, biometria, origem racial, religião, opinião política etc. Recebem proteção reforçada pela LGPD.
PII	Personally Identifiable Information — sinônimo de dado pessoal, conforme terminologia ISO 27018.
Titular dos dados	A pessoa a quem os dados se referem (ex.: colaborador, cliente, candidato, visitante).
Tratamento	Toda operação realizada com dados: coleta, uso, armazenamento, compartilhamento, eliminação e mais.

Termo	O que significa na prática
Controlador	A parte que decide como e por que os dados são tratados. A Surfix atua como Controladora dos dados de colaboradores, fornecedores, clientes e candidatos.
Operador (PII Processor)	Empresa ou pessoa que trata dados em nome do Controlador. A Surfix atua como Operadora no serviço Cloud Server (nuvem pública) para dados de clientes.
Encarregado (DPO)	Responsável por ser o canal entre a Surfix, os titulares de dados e a ANPD.
ANPD	Autoridade Nacional de Proteção de Dados — órgão público que fiscaliza o cumprimento da LGPD.
LGPD	Lei Geral de Proteção de Dados (Lei 13.709/2018) — legislação brasileira de privacidade.
Base legal	Justificativa legal que autoriza o tratamento de dados (ex.: contrato, obrigação legal, legítimo interesse).
Nuvem pública (Cloud Server)	Ambiente cloud compartilhado (multi-tenant) para múltiplos clientes. Serviço IaaS de instâncias em nuvem, conforme contrato.
Multi-tenancy	Arquitetura em que múltiplos clientes compartilham a mesma infraestrutura com segregação lógica entre ambientes.
ROPA	Registro de Operações de Tratamento — inventário de como os dados são tratados na organização.
RIPD / AIPD	Relatório de Impacto à Proteção de Dados — avaliação de riscos em tratamentos relevantes.

Princípios que guia o tratamento de dados:

Princípio	O que garantimos
Finalidade	Coletamos dados apenas para propósitos legítimos, específicos e informados.
Necessidade (Minimização)	Tratamos somente os dados estritamente necessários para cada finalidade.
Transparência	Informamos claramente quais dados coletamos, por que e como os usamos.
Segurança	Aplicamos controles técnicos e organizacionais para proteger os dados.
Prevenção	Adotamos medidas preventivas para evitar danos antes que ocorram.
Não discriminação	Dados sensíveis não são utilizados para fins discriminatórios.
Responsabilização	Mantemos registros que demonstram conformidade e prestamos contas quando solicitado.
Privacy by Design	A proteção de dados é considerada desde o início de qualquer projeto ou processo.
Privacy by Default	O maior nível de privacidade possível é aplicado por padrão em todas as configurações.
Rastreabilidade	Mantemos evidências de acesso, uso e tratamento de dados para fins de auditoria.

Incidentes de segurança: Em caso de incidente de segurança que envolva dados pessoais, a Surfix segue o seguinte fluxo.

#	Ação	Detalhe	Responsável
1	Identificar e comunicar o incidente	Comunicar imediatamente ao Comitê Gestor.	Quem identificou
2	Acionar o Plano de Resposta (P.GQ.14)	Conter o incidente e preservar evidências.	Comitê Gestor
3	Avaliar gravidade e impacto	Avaliar dados envolvidos, titulares afetados e risco.	Comitê Gestor
4	Notificar o Controlador	Prazo máximo: 72h após o reconhecimento. Informar: natureza dos dados, estimativa de titulares afetados e medidas adotadas.	DPO
5	Notificar a ANPD e, quando aplicável, o organismo certificador.	Quando aplicável — até 72h (recomendação ANPD).	DPO
6	Notificar os titulares afetados	Quando necessário e determinado pelo DPO.	DPO
7	Documentar e aprender	Registrar o incidente, ações e lições aprendidas.	Integrante do comitê Gestor

Quais dados tratamos e para quê? As tabelas a seguir detalham os dados coletados de cada grupo de titulares, finalidade, base legal e prazos de retenção.

Clientes:

Dados coletados	Contratante e representantes legais: nome, e-mail, telefone, CPF, RG/CNH e contrato social. Usuários indicados pelo cliente: nome, e-mail, telefone e registros de atendimento.
Para que usamos	Formalizar contratos, realizar cobranças e prestar suporte técnico.
Base legal (LGPD)	Art. 7º, V — Execução de contrato (dados operacionais/contratuais); Art. 7º, IX — Legítimo interesse, para comunicações da agência de marketing.
Compartilhado com	Bancos, sistemas internos, contabilidade, agência de marketing (com base no legítimo interesse — ver Base legal), departamento jurídico.

Fornecedores:

Dados coletados	Nome, e-mail e telefone do representante/responsável.
Para que usamos	Contato comercial, negociação e cotação, diligência e avaliação de fornecedores, formalização de contratos.
Base legal (LGPD)	Art. 7º, V — Execução de contrato.
Compartilhado com	Bancos, contabilidade, sistemas internos e departamento jurídico.

Candidatos a Vagas:

Dados coletados	Nome, telefone, e-mail, currículo, histórico profissional e vídeo de apresentação (imagem e voz). Documentos de identificação (RG, CPF) apenas na fase final, para viabilizar a contratação.
Para que usamos	Conduzir o processo seletivo, avaliar competências e viabilizar eventual contratação; manter o currículo em banco de talentos para oportunidades futuras, por até 18 meses caso não ocorra contratação.
Base legal (LGPD)	Art. 7º, V — procedimentos preliminares a contrato: processo seletivo e contratação. Art. 7º, IX — legítimo interesse: banco de talentos, com direito de oposição. O vídeo é usado só para avaliar comunicação e aderência à vaga.
Compartilhado com	Agência de estágio e consultoria de RH. Operadores que hospedam ou processam os dados: Microsoft Office 365.

Colaboradores e dependentes:

Dado pessoal	Finalidade	Base legal LGPD
Cadastrais e contratuais — nome, CPF, RG, endereço, CTPS, certidões, contrato, dados bancários	Admissão, folha, eSocial, obrigações trabalhistas, fiscais e previdenciárias	Obrigação legal — art. 7º, II; execução de contrato — art. 7º, V (dados bancários)
Saúde ocupacional — ASO, PCMSO, atestados	SST, justificativa de afastamentos, eSocial	Obrigação legal — art. 11, II, "a"; tutela da saúde — art. 11, II, "f", quando por profissional de saúde
Benefícios — dados do colaborador e dependentes, inclusive de saúde	Adesão e movimentação de plano de saúde e odontológico	Execução de contrato — art. 7º, V; consentimento específico e destacado — art. 11, I (dados de saúde); consentimento do responsável legal — art. 14, §1º (dependente criança ou adolescente).
Registros funcionais — histórico, avaliações, desenvolvimento	Gestão interna de pessoas	Legítimo interesse — art. 7º, IX
Biometria — ponto	Registro eletrônico de jornada	Obrigação legal — art. 11, II, "a"; prevenção à fraude — art. 11, II, "g"
Biometria — acesso físico	Controle de acesso a áreas restritas	Prevenção à fraude e segurança do titular — art. 11, II, "g"

ANEXO I – REQUISIÇÃO DOS TITULARES DE DADOS

Seus Direitos como Titular de Dados: A LGPD garante a você um conjunto de direitos sobre seus dados pessoais:

Direito	O que significa	Prazo de resposta
Confirmação de tratamento	Saber se tratamos seus dados.	Imediata, em formato simplificado
Acesso	Receber uma cópia dos seus dados (gratuita na 1ª solicitação).	Simplificada: Imediata Completa: até 15 dias corridos
Correção	Corrigir dados incompletos, inexatos ou desatualizados.	5 dias úteis
Anonimização Bloqueio Eliminação	Pedir que dados desnecessários ou irregulares sejam anonimizados, bloqueados ou excluídos.	15 dias corridos
Portabilidade	Receber seus dados em formato estruturado para uso em outro serviço.	15 dias corridos
Eliminação de dados tratados com consentimento	Pedir a exclusão dos dados tratados com base no seu consentimento.	15 dias corridos
Informação sobre compartilhamento	Saber com quais entidades públicas e privadas compartilhamos seus dados.	15 dias corridos
Informação sobre não consentir	Saber que você pode não fornecer consentimento e quais são as consequências dessa recusa.	Imediata, em formato simplificado
Revogação do consentimento	Retirar um consentimento dado anteriormente.	15 dias corridos
Oposição	Opor-se a determinado tratamento (ex.: comunicações de marketing).	15 dias corridos
Revisão de decisão automatizada	Solicitar revisão de decisões tomadas exclusivamente por sistemas automatizados.	15 dias corridos

IMPORTANTE:
COMO EXERCER SEUS DIREITOS:
lgpd@surfix.com.br | (81) 3419-8525 | Av. Eng. Domingos Ferreira, 2010 — Boa Viagem, Recife/PE — CEP 51.111-020
Formulário: Formulário de Requisição de Direitos do Titular de Dados Pessoais

A resposta simplificada informa se tratamos seus dados e quais categorias e finalidades estão envolvidas; a declaração completa indica origem, critérios e finalidade do tratamento. Os prazos contam a partir da confirmação da sua identidade.

Quando podemos negar uma solicitação?
Em situações específicas, uma solicitação pode ser parcial ou totalmente negada quando:

- Os dados foram anonimizados e não se enquadram mais como dados pessoais;
- Violaria os direitos de terceiros ou segredos da empresa;
- O tratamento é exigido por lei ou para exercício regular de direitos em processo judicial;

Em qualquer caso de negativa, informaremos os motivos de forma clara e por escrito.

ANEXO II – COMPARTILHAMENTO, TRANSFERENCIA E SUBCONTRATADOS

A Surfix compartilha dados pessoais apenas com parceiros necessários para a execução de suas atividades. Todo compartilhamento inclui cláusulas contratuais de segurança e confidencialidade.

Com quem compartilhamos:

- Instituições financeiras (bancos): para pagamentos e cobranças;
- Sistemas e plataformas tecnológicas (incluindo Microsoft Office 365): para viabilizar processos operacionais;
- Escritório de contabilidade: para cumprimento de obrigações fiscais;
- Agências de estágio e consultoria de RH: no processo de recrutamento;
- Departamento jurídico e tributário: para exercício regular de direitos;
- Agência de marketing: exclusivamente para comunicações autorizadas, com base no legítimo interesse (Art. 7º, IX da LGPD — ver Base legal na tabela de Clientes);
- Órgãos governamentais e certificadoras (ex.: certificações ISO, Receita Federal, ANPD, MTE): quando exigido por lei. Requisições governamentais ou judiciais de acesso a dados pessoais de clientes são tratadas conforme procedimento interno, sendo o Controlador notificado previamente sempre que permitido por lei.

Subcontratado (Subprocessador): fornecedor terceiro contratado pela Surfix para tratar dados pessoais em nome do cliente, dentro de um serviço já contratado. A LGPD (art. 5º, VII) trata esse fornecedor como um novo Operador. A Surfix só o inclui depois de avaliar sua segurança, exigir dele um compromisso de proteção de dados equivalente ao assumido com o cliente, e comunicar previamente essa inclusão ou troca — garantindo ao cliente o direito de se opor, conforme o art. 39 da LGPD.

Para os serviços prestados (ex.: cibersegurança gerenciada, e-mail corporativo e produtividade em nuvem), a Surfix pode subcontratar terceiros especializados para o tratamento de dados pessoais em nome do cliente-controlador, no âmbito da prestação do serviço contratado. Nenhum fornecedor é incorporado como subcontratado sem que, cumulativamente:

- Assuma obrigações contratuais de proteção de dados equivalentes às previstas no Contrato de Prestação de Serviços firmado com o cliente;
- Sua inclusão ou substituição seja comunicada ao cliente com antecedência mínima de 15 (quinze) dias, assegurado o direito de oposição motivada nesse prazo;
- Quando sediado ou processando dados fora do Brasil, a transferência observa as salvaguardas do art. 33 da LGPD.

Atualmente, os subcontratados que podem possuir alguma interação dados pessoais são:

Subcontratado	Serviço prestado / natureza do tratamento	Observações
Lumu Technologies	Cyber Threat Intelligence / monitoramento de rede (SaaS)	Fornecedor internacional — sujeito às salvaguardas do art. 33 da LGPD, quando aplicável.
SentinelOne	Proteção de endpoint — EPP/EDR/XDR (SaaS)	Fornecedor internacional — sujeito às salvaguardas do art. 33 da LGPD, quando aplicável.
Vicarius	Gestão de vulnerabilidades / patch management (SaaS)	Fornecedor internacional — sujeito às salvaguardas do art. 33 da LGPD, quando aplicável.
Skymail	E-mail corporativo (licenciamento/revenda)	Fornecedor hospeda e processa as caixas de e-mail licenciadas.

Esta relação é atualizada sempre que houver inclusão ou substituição de subcontratado, conforme o processo descrito nesta seção, e comunicada a atualização desta política as partes interessadas.

A relação de subcontratados pode ser ampliada ou alterada ao longo do tempo, desde que observado o processo descrito acima; avaliação de segurança, cláusula equivalente ao contrato e comunicação prévia.

No contexto do serviço Cloud Server (nuvem pública), o tratamento de dados pessoais é realizado em infraestrutura própria da Surfix. Não são utilizados suboperadores para tratamento de PII. Caso haja necessidade futura:

- A alteração estará sujeita a gestão de mudanças, avaliação de riscos e formalização contratual;
- O Controlador será notificado com antecedência mínima do prazo já relacionado acima;
- A Surfix manterá lista atualizada de suboperadores autorizados, disponível ao Controlador mediante solicitação;
- Suboperadores assumirão obrigações equivalentes às desta seção.

Transferências internacionais:
Dados podem ser armazenados ou processados no exterior em situações específicas, incluindo: (i) quando solicitado pelo próprio titular; (ii) por exigência de segurança nacional; ou (iii) no curso normal da prestação de serviços, quando subcontratados internacionais são utilizados para ferramentas de segurança e produtividade (ver relação de subcontratados no ANEXO II). Em todos os casos:

- O país ou parceiro destinatário deve oferecer nível de proteção compatível com a LGPD;
- São adotadas cláusulas contratuais padrão e garantias equivalentes às exigidas pela LGPD (art. 33);
- O armazenamento principal ocorre em servidores localizados no Brasil. Para o serviço Cloud Server (nuvem pública), os dados são armazenados em infraestrutura própria da Surfix no Brasil;
- O GDPR pode se aplicar caso a Surfix trate dados de titulares localizados na União Europeia; nesses casos, aplicam-se salvaguardas adicionais equivalentes às exigidas pela LGPD.

Treinamento e Conscientização:
A Surfix mantém um programa contínuo de treinamento e conscientização sobre privacidade e segurança da informação, incluindo temas específicos de nuvem. Todos os colaboradores devem:

- Participar dos treinamentos obrigatórios de privacidade, segurança, incluindo nuvem;
- Concluir curso e receber orientações antes de iniciar as atividades que envolvam o tratamento de dados;
- Participar de campanhas periódicas de conscientização;
- Ter participação registrada para fins de auditoria e comprovação de conformidade.

Objetivos de Segurança da Informação -
A Surfix estabelece objetivos de segurança da informação coerentes com esta política e com a direção estratégica da organização, mensuráveis sempre que possível, comunicados às partes interessadas relevantes e voltados à melhoria contínua do sistema de gestão. O monitoramento desses objetivos é feito por meio dos indicadores descritos a seguir.

Auditoria, monitoramento e indicadores:
Esta política e seus controles estão sujeitos a auditorias internas e externas periódicas, alinhadas aos ciclos de revisão das certificações a ela aplicada.

- Auditorias internas: realizadas periodicamente pelo auditor interno designado;
- Auditorias externas: realizadas por organismos certificadores ou parceiros autorizados;
- Indicadores: registros de treinamentos, prazo de resposta a titulares, número de incidentes, status do ROPA e conformidade dos controles cloud;
- Penalidades: o descumprimento desta política pode resultar em medidas disciplinares, contratuais, civis e penais.
  Casos Omissos: situações não previstas nesta política serão analisadas e deliberadas pelo Comitê Gestor de Segurança da Informação e Privacidade (CGSIP).

ANEXO lll Segurança e Privacidade em Nuvem (ISO 27017 / ISO 27018)

As diretrizes abaixo se aplicam aos serviços de computação em nuvem IaaS e SaaS abrangidos pelo escopo do SGSIP da Surfix.

Aplicabilidade das Normas de Nuvem:

ISO/IEC 27017	Aplicável aos serviços de computação em nuvem (IaaS e SaaS) contemplados pelo escopo SGSIP, conforme caracterização técnica e contratual vigente.
ISO/IEC 27018	Aplicável exclusivamente ao serviço Cloud Server, quando caracterizado como nuvem pública (multi-tenant) e quando a Surfix atuar como Operadora de Dados Pessoais (PII Processor). Não se aplica a colocation, servidores dedicados (bare metal), infraestrutura privada ou telecomunicações.
ROPA, RACI e DPA	Quando aplicável, os requisitos de privacidade e proteção de dados são implementados em conjunto com a Declaração de Aplicabilidade (SoA) e com os instrumentos de governança correlatos, assegurando coerência entre escopo, controles e responsabilidades.

Segurança da Informação: A Surfix adota controles técnicos e organizacionais para proteger os dados pessoais, em alinhamento com as normas aplicáveis.

Área de controle	Medidas adotadas
Política de SI	Diretrizes gerais de segurança da informação — papéis, responsabilidades e regras de uso de ativos.
Governança e acesso	MFA obrigatório para acessos administrativos, RBAC (menor privilégio), revisão periódica de acessos.
Criptografia	Dados protegidos em trânsito e em repouso, com algoritmos e gestão de chaves definidos na Política de Criptografia (POL.NC.02).
Endpoint e rede	Antivírus/EDR, firewall, segmentação de rede, VPN corporativa.
Backup & Recovery	Backups regulares com testes de restauração (P.DC.10).
Log & Monitoramento	Registro de atividades críticas com retenção conforme política vigente.
Desenvolvimento seguro	Conforme POL.GPI.01 — segurança desde a concepção (Privacy by Design).
Segurança física	Controle de acesso físico, câmeras de monitoramento e áreas restritas.
Nuvem (Cloud Server)	Controles de acesso e ferramentas aprovadas; segregação lógica multi-tenant com isolamento entre clientes (ISO 27018); links protegidos e permissões revisadas periodicamente.
BYOD	Regras de uso de dispositivos pessoais em atividades corporativas, com controles mínimos de segurança exigidos (POL.GQ.08).
Descarte Seguro	Descarte seguro conforme P.GA.08.

IMPORTANTE: A Surfix emprega seus melhores esforços para proteger os dados pessoais. No entanto, nenhuma transmissão pela internet é 100% segura. Em caso de incidente, a organização agirá com transparência e tomará as medidas corretivas necessárias.

Controles de Segurança em Nuvem (IaaS e SaaS):

Para os serviços IaaS e SaaS, a Surfix assegura, no mínimo:

- Modelo de responsabilidade compartilhada formalizado em contrato com o cliente;
- Segregação lógica de ambientes/tenants e separação de funções administrativas;
- Gestão de identidade e acessos (IAM) baseada em papéis, com princípio do menor privilégio, autenticação forte (MFA) e revisão periódica;
- Monitoramento e registro (logging) de atividades relevantes, com retenção, proteção e acesso controlado conforme SoA;
- Gestão de vulnerabilidades, hardening e aplicação de patches de segurança em prazos definidos por risco;
- Gestão segura de APIs e interfaces administrativas (autenticação, autorização e controle de exposição);
- Gestão de mudanças controlada, com avaliação de risco, aprovação, registro e plano de reversão;
- Continuidade de negócios para serviços em nuvem conforme PCN e SLAs/RTO/RPO acordados;
- Gestão de fornecedores relacionados ao serviço (ex.: conectividade, hardware, software).

Proteção de Dados Pessoais em Nuvem — Obrigações da Surfix como Operadora:

Nos serviços em que a Surfix atua como Operadora de Dados Pessoais do cliente (Controlador) — incluindo, entre outros, Cloud Server (nuvem pública), IaaS, SaaS e Backup —, aplica-se:

- Tratar dados pessoais (PII) exclusivamente conforme instruções documentadas do cliente (Controlador), sem utilizá-los para finalidade própria (incluindo marketing, perfilamento ou analytics não autorizado);
- Garantir controles de acesso a PII, incluindo acesso privilegiado restrito, rastreável e auditável;
- Aplicar criptografia em repouso para PII;
- Preservar segregação lógica (multi-tenant) e mitigar riscos de acesso indevido entre clientes;
- Apoiar o Controlador no atendimento aos direitos dos titulares, fornecendo suporte técnico no prazo máximo de 5 dias úteis;
- Notificar incidentes envolvendo PII ao Controlador no prazo máximo de 72 horas após o reconhecimento, informando: natureza dos dados, estimativa de titulares afetados e medidas adotadas;
- Assegurar retenção, devolução e exclusão segura de PII: prazo máximo de 30 dias após término do contrato, com certificado de destruição quando solicitado; dados disponibilizados em formato aberto por mínimo de 90 dias após encerramento (ISO 27018);
- Requisições governamentais ou judiciais de acesso a dados pessoais de clientes são tratadas conforme procedimento interno, sendo o Controlador notificado previamente sempre que permitido por lei.

Gestão de Riscos, Incidentes, Mudanças e Continuidade em Nuvem:

Gestão de riscos	Realizada de forma sistemática e integrada ao SGSIP, com identificação, avaliação, tratamento e monitoramento de riscos específicos de nuvem, conforme processos internos e SoA vigente.
Gestão de incidentes	Incidentes de segurança e privacidade em nuvem seguem o processo interno de gerenciamento de incidentes (P.GQ.14). Incidentes com PII seguem as obrigações descritas nas seções "Proteção de Dados Pessoais em Nuvem — Obrigações da Surfix como Operadora" e "Incidentes de segurança" desta política.
Gestão de mudanças	Mudanças que impactem serviços em nuvem são avaliadas quanto a risco e impacto, aprovadas, implementadas e registradas de forma controlada (GMUD).
Continuidade	O PCN é mantido e testado periodicamente, assegurando RTO/RPO acordados contratualmente.

Ciclo de Vida dos Dados:

Etapa	O que fazemos
Registro e Catalogação	Mantemos o ROPA atualizado (D.GQ.57) com o inventário de todos os tratamentos.
Uso e Compartilhamento	Dados utilizados somente para a finalidade original; qualquer compartilhamento é registrado.
Armazenamento	Dados armazenados em repositórios autorizados, com controles de acesso e criptografia.
Retenção	Mantidos pelos prazos definidos nesta política (seção “Quais dados tratamos e para quê?”) ou conforme obrigação legal.
Eliminação	Ao término do prazo ou por instrução do Controlador, os dados são eliminados de forma segura e auditável no prazo máximo de 30 dias, com emissão de certificado de destruição quando solicitado. Para o Cloud Server: dados em formato aberto disponíveis por mínimo de 90 dias após encerramento.

Disposições finais:

Esta política entra em vigor a partir da data da sua publicação e será revisada a cada 24 meses, ou sempre que houver alteração legal, regulatória ou organizacional relevante, ou incidente relevante de segurança da informação.

Aplica-se à República Federativa do Brasil, regida pela Lei 13.709/2018 (LGPD), sendo competente o foro de Recife/PE.

Esta política não substitui acordos de confidencialidade firmados individualmente, mas deve ser lida em conjunto com eles.