

SUMÁRIO:

1.	Declaração da liderança	2
2.	Para que serve esta política	2
3.	Segurança e privacidade: o que cada uma cobre.....	2
4.	Onde esta política se aplica	2
5.	Quem é responsável	3
6.	Termos usados neste documento	3
7.	Diretrizes de segurança da informação	4
8.	Diretrizes de privacidade	5
9.	Quais dados tratamos, para quê e por quanto tempo.....	6
10.	Com quem compartilhamos e transferência internacional.....	7
11.	Seus direitos como titular de dados	8
12.	Quando a Surfix trata dados em nome do cliente (Operadora e nuvem)	8
13.	Incidentes de segurança e privacidade.....	9
14.	Pessoas, objetivos e auditoria.....	9
15.	Descumprimento e casos omissos.....	10
16.	Vigência e revisão	10

1. Declaração da liderança:

A alta direção da Surfix Cloud & Data Center declara que a segurança da informação e a privacidade são pilares do negócio. Proteger as informações e os dados pessoais contra acesso indevido, vazamento, fraude, perda e indisponibilidade é essencial para manter os serviços funcionando, cumprir a lei e preservar a confiança de clientes, parceiros e colaboradores.

A direção se compromete a: cumprir a LGPD, os contratos e as demais exigências legais, regulatórias e normativas aplicáveis; manter e melhorar continuamente o Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP); prover os recursos necessários; e tratar esta política como obrigação de toda a organização, não apenas da área de tecnologia.

2. Para que serve esta política?

Esta política define as diretrizes de segurança da informação, privacidade e segurança em nuvem da Surfix. Ela é pública e se dirige a clientes, titulares de dados, fornecedores, parceiros, órgãos reguladores e organismos de certificação. As regras de conduta para colaboradores e para terceiros que atuam em nome da Surfix estão na **Política Interna de Segurança da Informação e Privacidade (POL.GQ.02)**, que complementa esta política e não a contradiz.

Seu objetivo é garantir a confidencialidade, a integridade e a disponibilidade das informações e dos dados pessoais sob responsabilidade da Surfix; atender aos requisitos legais, regulatórios e contratuais; apoiar a continuidade do negócio e a gestão de riscos; prevenir incidentes; e promover uma cultura de segurança e privacidade.

Para os titulares de dados, esta política também funciona como aviso de privacidade (art. 9º da LGPD): ela informa quais dados tratamos, para quê, com quem compartilhamos, por quanto tempo guardamos e como exercer seus direitos. A partir desta revisão, ela substitui os documentos POL.GQ.03, POL.GQ.05, POL.GQ.12 e POL.GQ.13.

3. Segurança e privacidade: o que cada uma cobre:

Segurança da informação e privacidade se complementam, mas não são a mesma coisa. Esta política trata das duas e deixa claro onde uma vai além da outra.

A segurança vai além da privacidade. A segurança protege toda informação da Surfix e de seus clientes, não só os dados pessoais. Isso inclui contratos, dados financeiros, configurações de rede, credenciais, códigos, registros de sistema (logs), backups e a própria disponibilidade dos serviços de data center e nuvem. Um servidor de cliente sem nenhum dado pessoal continua protegido pelas mesmas regras.

A privacidade vai além da segurança. Proteger o dado não basta. Um dado pessoal pode estar perfeitamente seguro e, ainda assim, ser tratado de forma ilegal: coletado sem finalidade clara, usado para outro fim, guardado por mais tempo que o necessário, compartilhado sem base legal ou sem que o titular saiba. A privacidade exige finalidade, base legal, transparência, mínimo de dados, prazo de guarda e respeito aos direitos do titular.

Por isso, as diretrizes de segurança (seção 7) valem para toda informação, e as diretrizes de privacidade (seção 8) valem sempre que houver dado pessoal. Quando as duas se aplicam ao mesmo caso, prevalece a regra que mais protege a informação e o titular.

4. Onde esta política se aplica?

O SGSIP da Surfix cobre os serviços de data center, colocation, servidores dedicados, Cloud Server (nuvem pública), backup, segurança gerenciada e e-mail corporativo, conforme a Declaração de Escopo do SGSIP vigente. Estão dentro do escopo os dados pessoais de colaboradores, dependentes, candidatos e representantes de clientes e fornecedores (Surfix como Controladora) e os dados pessoais contidos nos ambientes dos clientes (Surfix como Operadora).

Público	Como esta política se aplica
Clientes e usuários	Em todo o ciclo comercial: proposta, contrato, suporte e encerramento, junto com o contrato e os termos de uso.
Titulares de dados	Como aviso de privacidade: quais dados tratamos, para quê, por quanto tempo e como exercer direitos.
Fornecedores e parceiros	Como referência das exigências de segurança e privacidade incluídas nos contratos.
ANPD, órgãos públicos e certificadoras	Como fonte pública das diretrizes, dos responsáveis e dos canais de contato.

Público	Como esta política se aplica
Colaboradores e terceiros que atuam em nome da Surfix	Esta política e, além dela, a POL.GQ.02, com as regras do dia a dia.

Esta política é pública e fica disponível em [Início - Surfix Cloud & Data Center](#)

5. Quem é responsável?

Encarregada de Dados (DPO): Patrícia Fracassio — lgpd@surfix.com.br | (81) 3419-8525 | Av. Eng. Domingos Ferreira, 2010 — Boa Viagem, Recife/PE — CEP 51.111-020. A Encarregada é o canal entre a Surfix, os titulares e a ANPD (art. 41 da LGPD) e atua com autonomia para exercer essa função.

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).

Quem	O que faz
Alta direção	Aprova esta política, fornece recursos, define o apetite ao risco e analisa criticamente o SGSIP ao menos uma vez por ano.
Encarregada (DPO)	Atende titulares e a ANPD; orienta as áreas; acompanha a conformidade; decide sobre notificações de incidente com dados pessoais.
CGSIP	Mantém o inventário de tratamentos (ROPA) e a Declaração de Aplicabilidade (SoA); avalia riscos, contratos, fornecedores e provedores; implementa e audita controles; conduz incidentes.
Colaboradores e terceiros em nome da Surfix	Cumprem esta política e a POL.GQ.02; fazem os treinamentos; reportam incidentes imediatamente.
Fornecedores e prestadores	Tratam informações conforme o contrato; notificam a Surfix em caso de incidente; não subcontratam o tratamento de dados pessoais sem autorização prévia e por escrito.
Clientes (Controladores)	Definem, por contrato, as instruções de tratamento dos dados que hospedam na Surfix e respondem pela base legal desses dados.

6. Termos usados neste documento:

Termo	O que significa na prática
Informação / ativo	Qualquer dado com valor para a Surfix ou seus clientes, em qualquer formato: arquivo, e-mail, sistema, servidor, backup, contrato, configuração.
Incidente	Qualquer evento que comprometa, ou possa comprometer, a confidencialidade, a integridade ou a disponibilidade de uma informação (ex.: vazamento, invasão, perda, indisponibilidade).
Dado pessoal (PII)	Informação que identifica ou pode identificar uma pessoa (nome, CPF, e-mail, telefone, IP). PII é o termo usado pelas normas ISO.
Dado sensível	Dado sobre saúde, biometria, origem racial, religião, opinião política, vida sexual e similares. Tem proteção reforçada (art. 11 da LGPD).
Titular	A pessoa a quem o dado se refere (colaborador, cliente, candidato, visitante).
Tratamento	Toda operação com dado pessoal: coleta, uso, acesso, armazenamento, compartilhamento, eliminação.
Controlador	Quem decide como e por que os dados são tratados. A Surfix é Controladora dos dados de colaboradores, candidatos, clientes e fornecedores.
Operador	Quem trata dados em nome do Controlador, seguindo suas instruções. A Surfix é Operadora dos dados que os clientes hospedam em seus serviços.

Termo	O que significa na prática
Suboperador	Fornecedor contratado pela Surfix para tratar dados pessoais em nome do cliente, dentro de um serviço já contratado.
ANPD	Autoridade Nacional de Proteção de Dados — agência que fiscaliza a LGPD.
Base legal	A hipótese da LGPD que autoriza o tratamento (ex.: contrato, obrigação legal, legítimo interesse, consentimento).
ROPA	Registro das Operações de Tratamento — inventário de quais dados tratamos, de quem, para quê, onde e por quanto tempo.
RIPD	Relatório de Impacto à Proteção de Dados — avaliação dos riscos ao titular em tratamentos de maior risco.
SoA	Declaração de Aplicabilidade — lista dos controles das normas ISO que a Surfix adota e a justificativa dos não adotados.
Cloud Server / multi-tenant	Serviço de nuvem pública da Surfix em que vários clientes compartilham a mesma infraestrutura, com separação lógica entre eles.

7. Diretrizes de segurança da informação:

A Surfix protege a informação em três aspectos: **confidencialidade** (só quem precisa acessa), **integridade** (a informação está correta e completa) e **disponibilidade** (a informação está acessível quando necessária). A Surfix classifica a informação, avalia os riscos de segurança e de privacidade ao menos uma vez por ano e sempre que houver mudança relevante, e registra os controles adotados na Declaração de Aplicabilidade (SoA). As principais medidas são:

Área	O que fazemos
Acesso	Cada pessoa acessa só o que precisa para sua função (menor privilégio). Acessos administrativos exigem autenticação em dois fatores (MFA) quando haver aplicabilidade no sistema. Os acessos são revisados periodicamente a cada 03 meses em auditoria interna e removidos no desligamento e/ou distrato.
Criptografia	Dados protegidos em trânsito e em repouso, com algoritmos e gestão de chaves definidos em política própria.
Endpoint e rede	Antivírus/EDR, firewall, segmentação de rede e VPN corporativa.
Backup e recuperação	Backups regulares, com testes de restauração.
Registro e monitoramento	Atividades críticas são registradas (logs), protegidas e guardadas pelo prazo definido.
Vulnerabilidades e mudanças	Correções de segurança aplicadas em prazos definidos por risco. Mudanças são avaliadas, aprovadas, registradas e têm plano de retorno.
Desenvolvimento seguro	Segurança e privacidade consideradas desde a concepção de sistemas e serviços.
Segurança física	Controle de acesso físico, câmeras e áreas restritas no data center e nos escritórios.
Fornecedores	Fornecedores com acesso a informações ou dados pessoais são avaliados antes da contratação e assinam cláusulas de segurança e confidencialidade.
Continuidade	Plano de Continuidade de Negócios (PCN) mantido e testado, com tempos de recuperação (RTO/RPO) acordados em contrato.
Pessoas	Colaboradores e terceiros seguem regras de uso aceitável, senhas, dispositivos e manuseio de informação (POL.GQ.02) e são treinados antes de acessar informações de clientes.
Descarte seguro	Mídias, equipamentos e documentos são descartados de forma que a informação não possa ser recuperada.

Área	O que fazemos
Incidentes	Todo incidente é tratado, registrado e analisado (seção 13).

8. Diretrizes de privacidade:

Sempre que houver dado pessoal, a Surfix segue os princípios da LGPD (art. 6º):

Princípio	O que garantimos
Finalidade e adequação	Coletamos dados para propósitos legítimos, específicos e informados, e usamos de forma compatível com esses propósitos.
Necessidade	Tratamos somente o mínimo de dados necessário para cada finalidade.
Livre acesso e transparência	O titular pode saber, de forma fácil e gratuita, quais dados temos, por que e como os usamos.
Qualidade	Mantemos os dados exatos, claros e atualizados.
Segurança e prevenção	Aplicamos medidas técnicas e organizacionais para proteger os dados e evitar danos antes que ocorram.
Não discriminação	Não usamos dados para fins discriminatórios ou abusivos.
Responsabilização	Mantemos registros que demonstram conformidade e prestamos contas quando solicitado.
Privacidade desde a concepção e por padrão	A proteção de dados é considerada desde o início de todo projeto, sistema ou serviço, e a configuração mais protetiva é a padrão.

Como aplicamos. Todo tratamento tem uma base legal registrada no ROPA. O consentimento só é usado quando nenhuma outra base serve e pode ser revogado a qualquer momento. Novos projetos, sistemas e serviços passam por avaliação de privacidade antes de entrar em operação. Quando o tratamento puder gerar risco alto ao titular, a Surfix elabora um RIPD (art. 38 da LGPD). A avaliação de riscos considera o risco para o titular, e não apenas para a empresa. Dados sensíveis e dados de crianças e adolescentes são tratados somente nas hipóteses dos arts. 11 e 14 da LGPD e no melhor interesse do menor. A Surfix não toma decisões exclusivamente automatizadas que afetem os interesses dos titulares; se vier a adotá-las, garantirá o direito de revisão (art. 20).

Etapas do ciclo de vida	O que fazemos
Registro	Mantemos o ROPA atualizado com o inventário de todos os tratamentos.
Uso e compartilhamento	Dados usados somente para a finalidade original. Todo compartilhamento tem base legal e é registrado.
Armazenamento	Dados guardados em repositórios autorizados, com controle de acesso e criptografia.
Retenção	Dados mantidos pelos prazos da seção 9 ou pelo prazo exigido por lei.
Eliminação	Ao fim do prazo, ou por instrução do Controlador, os dados são eliminados de forma segura e registrada em até 30 dias.

9. Quais dados tratamos, para quê e por quanto tempo?

As tabelas abaixo valem para os dados em que a Surfix é Controladora. Os dados hospedados pelos clientes nos serviços da Surfix seguem a seção 12. Os dados de colaboradores e dependentes são informados a eles no aviso de privacidade interno (POL.GQ.02).

Clientes (representantes e contatos):

Dados coletados	Nome, e-mail, telefone, CPF, RG/CNH e cópia do contrato social.
Para que usamos	Formalizar contratos, emitir cobranças, prestar suporte técnico e enviar comunicações sobre os serviços.
Base legal	Execução de contrato (art. 7º, V). Legítimo interesse para comunicações comerciais (art. 7º, IX), com direito de oposição.
Compartilhado com	Bancos, sistemas internos, contabilidade, departamento jurídico e agência de marketing de acordo com a seção 10.
Por quanto tempo	Durante o contrato e por 5 anos após o encerramento, para defesa em eventuais processos e novas oportunidades de negócios. Exceto quando solicitado pelo cliente de acordo com a seção 11 e com finalidade apresentada.

Fornecedores (representantes e contatos):

Dados coletados	Nome, e-mail e telefone do representante.
Para que usamos	Compras, negociação, avaliação de fornecedores e formalização de contratos.
Base legal	Execução de contrato (art. 7º, V).
Por quanto tempo	Durante o contrato e por 5 anos após o encerramento e para defesa em eventuais processos. Exceto quando solicitado pelo fornecedor de acordo com a seção 11 e com finalidade apresentada.

Candidatos a vagas:

Dados coletados	Nome, telefone, e-mail, currículo, histórico profissional, documentos e vídeo de apresentação.
Para que usamos	Conduzir o processo seletivo, avaliar competências e viabilizar a contratação.
Base legal	Procedimentos preliminares ao contrato (art. 7º, V) e legítimo interesse (art. 7º, IX).
Compartilhado com	Agência de estágio, consultoria de RH e plataforma Microsoft 365.
Por quanto tempo	Até 18 meses após o fim do processo seletivo, caso não haja contratação. Exceto quando solicitado pelo candidato de acordo com a seção 11 e com finalidade apresentada.

10. Com quem compartilhamos e transferência internacional:

A Surfix compartilha dados pessoais apenas com quem é necessário para executar suas atividades. Todo compartilhamento tem base legal, cláusulas contratuais de segurança e confidencialidade e é registrado no ROPA. Compartilhamos com: instituições financeiras (pagamentos e cobranças); plataformas tecnológicas (inclusive Microsoft 365); escritório de contabilidade; agências de estágio e consultoria de RH; departamento jurídico e tributário; agência de marketing (comunicações autorizadas); e órgãos públicos e certificadoras (Receita Federal, ANPD, MTE, organismos de certificação ISO), quando exigido por lei.

Requisições de autoridades públicas ou judiciais para acesso a dados de clientes seguem procedimento interno, são registradas e, sempre que a lei permitir, o cliente Controlador é avisado antes.

Suboperadores. A Surfix pode contratar terceiros para tratar dados pessoais em nome do cliente dentro de um serviço contratado (ex.: segurança gerenciada, e-mail corporativo). Nenhum suboperador é incluído sem que, ao mesmo tempo: (i) tenha sua segurança avaliada; (ii) assuma por contrato obrigações de proteção de dados equivalentes às assumidas com o cliente; e (iii) sua inclusão ou troca seja comunicada ao cliente com ao menos 15 dias de antecedência, com direito de oposição motivada nesse prazo. Quando o suboperador estiver fora do Brasil, aplicam-se as regras de transferência internacional desta seção. Os suboperadores atuais são:

Suboperador	Serviço / natureza do tratamento	Observação
Lumu Technologies	Inteligência de ameaças e monitoramento de rede (SaaS)	Internacional — salvaguardas do art. 33 da LGPD

Suboperador	Serviço / natureza do tratamento	Observação
SentinelOne	Proteção de endpoint — EPP/EDR/XDR (SaaS)	Internacional — salvaguardas do art. 33 da LGPD
Vicarius	Gestão de vulnerabilidades e patches (SaaS)	Internacional — salvaguardas do art. 33 da LGPD
Skymail	E-mail corporativo (licenciamento e revenda)	Hospeda e processa as caixas de e-mail licenciadas
Microsoft	Microsoft 365 — produtividade e colaboração	Internacional — salvaguardas do art. 33 da LGPD

No serviço Cloud Server (nuvem pública), o tratamento ocorre em infraestrutura própria da Surfix no Brasil, sem suboperadores. Qualquer inclusão futura seguirá gestão de mudanças, avaliação de riscos, formalização contratual e o aviso prévio acima. A lista de suboperadores é atualizada a cada inclusão ou troca e fica disponível ao cliente nesta política e mediante solicitação.

Transferência internacional. O armazenamento principal dos dados ocorre em servidores no Brasil. Dados podem ser tratados no exterior apenas: (i) quando o próprio titular solicitar ou consentir de forma específica; ou (ii) no curso normal dos serviços, por meio dos suboperadores internacionais listados acima. Em todos os casos, a Surfix usa um dos mecanismos do art. 33 da LGPD: país com nível de proteção reconhecido pela ANPD (a União Europeia é reconhecida pela Resolução CD/ANPD nº 32/2026), cláusulas-padrão contratuais aprovadas pela ANPD (Resolução CD/ANPD nº 19/2024) ou outra garantia equivalente. Se a Surfix tratar dados de pessoas localizadas na União Europeia, o GDPR pode se aplicar e salvaguardas adicionais são adotadas.

11. Seus direitos como titular de dados:

A LGPD (art. 18) garante ao titular os direitos abaixo. Para exercê-los, envie um e-mail para lgpd@surfix.com.br. A Surfix pode pedir comprovação de identidade antes de atender, para que os dados não sejam entregues a outra pessoa. O atendimento é gratuito.

Direito	O que significa	Prazo de resposta
Confirmação e acesso	Saber se tratamos seus dados e receber uma cópia deles.	Confirmação simples: até 5 dias úteis. Cópia completa: até 15 dias (art. 19).
Correção	Corrigir dados incompletos, inexatos ou desatualizados.	Até 5 dias úteis
Anonimização, bloqueio ou eliminação	Pedir que dados desnecessários, excessivos ou tratados de forma irregular sejam anonimizados, bloqueados ou eliminados.	Até 15 dias
Portabilidade	Receber seus dados em formato estruturado para uso em outro serviço.	Até 15 dias
Informação sobre compartilhamento	Saber com quais entidades públicas e privadas compartilhamos seus dados.	Até 15 dias
Informação sobre o consentimento	Saber que pode não consentir e quais as consequências da negativa.	Até 15 dias
Revogação do consentimento e eliminação	Retirar um consentimento dado e pedir a exclusão dos dados tratados com base nele.	Até 15 dias
Oposição	Opor-se a um tratamento feito sem consentimento (ex.: comunicações de marketing).	Até 15 dias
Revisão de decisão automatizada	Pedir revisão de decisão tomada só por sistemas automatizados.	Até 15 dias

Quando um pedido pode ser negado. Um pedido pode ser negado, no todo ou em parte, quando os dados já foram anonimizados; quando atendê-lo violar direitos de terceiros ou segredo de negócio; quando a guarda for exigida por lei, contrato ou para exercício de direitos em processo; ou quando o legítimo interesse da Surfix prevalecer, de forma justificada. Toda negativa é informada por escrito, com os motivos. O titular pode, a qualquer tempo, apresentar reclamação à ANPD (gov.br/anpd).

12. Quando a Surfix trata dados em nome do cliente (Operadora e nuvem)?

Nos serviços em que o cliente hospeda dados na Surfix — Cloud Server, IaaS, SaaS, backup, segurança gerenciada e e-mail —, o cliente é o Controlador e a Surfix é a Operadora. A Surfix aplica a ISO/IEC 27017 a todos os serviços de nuvem do escopo e a ISO/IEC 27018 ao Cloud Server, quando opera como nuvem pública multi-tenant. A ISO/IEC 27018 não se aplica a colocation, servidores dedicados, infraestrutura privada ou telecomunicações.

Obrigações da Surfix como Operadora. A Surfix:

- Trata os dados apenas conforme as instruções documentadas do cliente, definidas em contrato, e nunca para finalidade própria (marketing, perfilamento ou análise não autorizada).
- Avisa o cliente, antes de executar, se uma instrução recebida violar a LGPD ou outra lei.
- Mantém registro dos tratamentos feitos em nome de cada cliente e o disponibiliza quando solicitado.
- Restringe o acesso privilegiado aos ambientes do cliente a pessoas autorizadas, com registro e possibilidade de auditoria.
- Aplica criptografia de acordo com a política interna da Surfix.
- Mantém a separação lógica entre clientes (multi-tenant) e trata os riscos de acesso indevido entre eles.
- Apoia o cliente no atendimento aos direitos dos titulares, com suporte técnico em até 5 dias úteis.
- Notifica o cliente sobre incidentes com dados pessoais em até 72 horas após o conhecimento, informando natureza dos dados, estimativa de titulares afetados e medidas adotadas.
- Ao fim do contrato, mantém os dados disponíveis para exportação em formato aberto por ao menos 90 dias e, depois, os elimina de forma segura em até 30 dias.
- Comunica previamente a inclusão ou troca de suboperadores e as transferências internacionais, conforme a seção 10.
- Formaliza com o cliente o modelo de responsabilidade compartilhada: o que a Surfix protege e o que cabe ao cliente proteger.

Controles de nuvem. Para os serviços IaaS e SaaS, a Surfix mantém separação de funções administrativas; gestão de identidades por papéis, com MFA e revisão periódica; registro e monitoramento das atividades relevantes, com guarda e acesso controlados; gestão de vulnerabilidades, hardening e patches; proteção de APIs e interfaces administrativas; gestão de mudanças controlada; continuidade conforme PCN e os RTO/RPO contratados; e gestão dos fornecedores do serviço (conectividade, hardware e software). Os riscos específicos de nuvem são avaliados e tratados junto com os demais riscos do SGSIP.

A Surfix emprega seus melhores esforços para proteger os dados. Nenhuma transmissão pela internet é 100% segura. Em caso de incidente, a Surfix age com transparência e adota as medidas corretivas necessárias.

13. Incidentes de segurança e privacidade:

Todo incidente de segurança, com ou sem dado pessoal, segue o Plano de Resposta a Incidentes da Surfix. Clientes, titulares e parceiros que suspeitem de um incidente podem comunicá-lo pelo canal de suporte ou por lgpd@surfix.com.br. Quando o incidente envolve dado pessoal, a Surfix segue este fluxo:

Passo	Ação	Detalhe	Responsável
1	Identificar e comunicar	Comunicar imediatamente pelos canais internos ou externos de suporte.	Quem identificou
2	Conter e preservar	Conter o incidente e preservar as evidências.	CGSI
3	Avaliar gravidade	Avaliar dados envolvidos, titulares afetados, causa e risco de dano.	DPO + CGSI

Passo	Ação	Detalhe	Responsável
4	Notificar o cliente Controlador	Quando a Surfix for Operadora: em até 72 horas após o conhecimento, com natureza dos dados, estimativa de titulares afetados e medidas adotadas.	DPO
5	Notificar a ANPD	Quando houver risco ou dano relevante aos titulares: em até 3 dias úteis após o conhecimento (art. 48 da LGPD e Resolução CD/ANPD nº 15/2024). Avisar o organismo certificador quando o contrato exigir.	DPO
6	Notificar os titulares	No mesmo prazo da ANPD, quando houver risco ou dano relevante, em linguagem simples.	DPO
7	Registrar e aprender	Registrar o incidente, as ações e as lições aprendidas. Abrir ação corretiva quando necessário.	CGSI + DPO

14. Pessoas, objetivos e auditoria:

Todo colaborador e terceiro que atua em nome da Surfix é treinado em segurança da informação e privacidade antes de acessar informações de clientes ou dados pessoais, e ao menos uma vez por ano. A Surfix define objetivos de segurança da informação e privacidade coerentes com esta política, mensuráveis sempre que possível, com responsável e prazo, e os revisa na análise crítica do SGSIP. O acompanhamento usa indicadores como conclusão dos treinamentos, prazo de resposta aos titulares, número e tempo de tratamento de incidentes, atualização do ROPA e conformidade dos controles de nuvem. Esta política e seus controles passam por auditorias internas e por auditorias externas dos organismos certificadores, nos ciclos das certificações.

15. Descumprimento e casos omissos:

O descumprimento desta política por colaboradores, fornecedores ou parceiros pode resultar em medidas disciplinares, contratuais, civis e penais, conforme o caso. Situações não previstas aqui são decididas pelo CGSI, com apoio da DPO quando houver dado pessoal.

16. Vigência e revisão:

Esta política entra em vigor na data de publicação. Ela é revisada no máximo a cada 24 meses ou antes, sempre que houver mudança legal, regulatória, contratual ou organizacional relevante, ou incidente relevante. Cada revisão é aprovada pela direção e comunicada aos colaboradores, terceiros e clientes.

Esta política é regida pela legislação brasileira, em especial a LGPD (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 12.737/2012, e segue as normas ISO/IEC 27001, 27701, 27017 e 27018. Fica eleito o foro de Recife/PE. Esta política não substitui os acordos de confidencialidade firmados individualmente e deve ser lida em conjunto com eles.