swile

Whitepaper de Segurança da Informação

2026

Table of contents

01.

Introdução

O objetivo deste documento é fornecer informações de alto nível aos nossos clientes e a todas as partes interessadas sobre o compromisso da Swile com a confiança digital, incluindo segurança, ética de dados e privacidade, continuidade de negócios e governança.

Compromisso Corporativo de Confiança da Swile

A Swile está comprometida em conquistar e manter a confiança de nossos clientes. Nosso objetivo é ser o mais transparente possível com nossos clientes, oferecendo segurança e proteções de ponta para atender e superar as expectativas de nossos clientes.

Nossos compromissos

- **Garantir a integridade** das transações, das pessoas e dos dados pessoais
- **Respeitar a privacidade** e fazer uso justo dos dados pessoais
- **Trabalhar continuamente para melhorar a confiabilidade e a continuidade de nossos serviços**
- **Buscar o mais alto nível de qualidade de governança** em relação à segurança e à privacidade ao longo de todo o ciclo de vida dos dados
- **Monitorar e comunicar de forma transparente** nossas conquistas em Confiança Digital

Governança de Segurança da Swile

O CISO da Swile é responsável por todas as atividades de Confiança Digital dos Serviços da Swile, incluindo supervisão e responsabilização. O CISO é apoiado por especialistas em privacidade, fraude e compliance das áreas jurídica e financeira.

A Swile possui uma equipe dedicada responsável pelas operações de segurança, encarregada de:

- Conscientização dos usuários e antecipação de ameaças
- Endurecimento (hardening) e proteção de dispositivos e softwares do sistema de informação
- Controles de segurança e testes ofensivos
- Monitoramento, detecção e resposta a tentativas de intrusão
- Resposta a incidentes

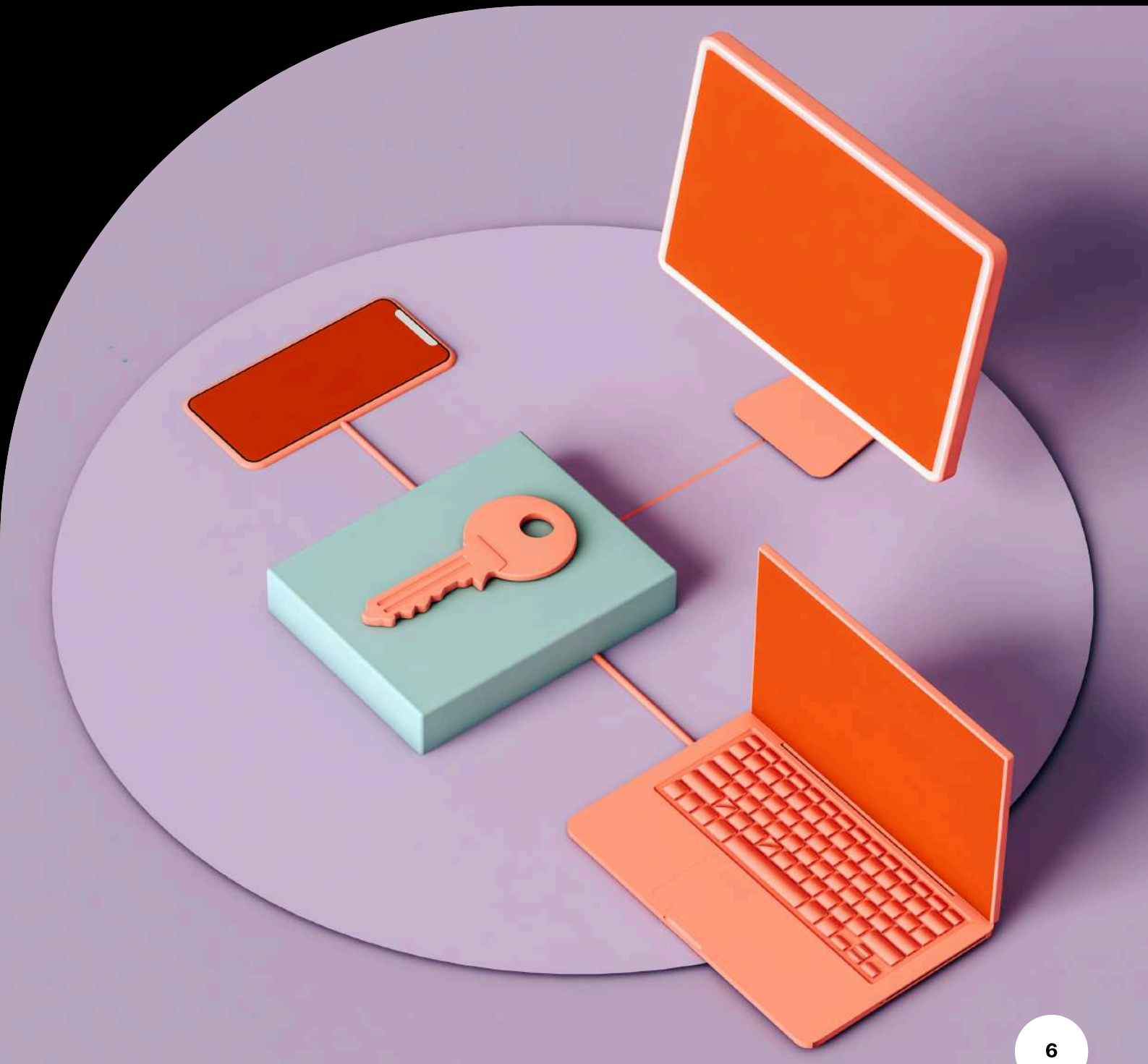
Os contratos da Swile com provedores de hospedagem terceirizados, como a Amazon Web Services, incluem requisitos de proteção da informação alinhados às práticas do setor.

Com base em normas ISO, a Swile estabeleceu uma organização e uma governança de segurança com liderança executiva de segurança, responsáveis de segurança e especialistas técnicos envolvidos nas operações diárias.

A Swile possui uma política de segurança da informação documentada, que é ativamente revisada e atualizada. O desenvolvimento, a manutenção e a publicação da política de segurança são de responsabilidade do CISO da Swile. Qualquer violação dessa política pode ser sancionada por medidas disciplinares e/ou ações judiciais.

02.

Qualidade de serviço e continuidade de negócios



2.1

Infraestrutura da Swile e arquitetura de terceiros

A Swile hospeda sua infraestrutura em datacenters da Amazon Web Services (AWS). Para clientes europeus, os dados são hospedados na França.

A Swile utiliza alguns serviços de terceiros, como processadores de pagamento ou serviços de roteamento de e-mail. A contratação desses provedores está sujeita a uma análise de práticas de segurança para garantir a conformidade com nossa política de segurança e com as regulamentações vigentes.

Nossos contratos com esses suboperadores incluem cláusulas de segurança, especialmente no que diz respeito à proteção de dados pessoais.

2.2

Confiabilidade e backup

2.2.1
Alta disponibilidade por design

Desde a concepção, a Swile implementou uma infraestrutura de alta disponibilidade:

- A plataforma da Swile possui redundâncias incorporadas em todos os níveis do serviço.
- A infraestrutura da Swile é implantada em múltiplas zonas de disponibilidade da AWS localizadas na França (ou seja, em vários datacenters independentes).
- A plataforma é disponibilizada por meio de balanceadores de carga redundantes, que direcionam o tráfego para a infraestrutura de serviços (por exemplo, servidores web).
- Os dados são replicados em múltiplos servidores de banco de dados, localizados em diferentes datacenters da AWS.
- Os storages dos servidores são protegidos contra perda por meio de um sistema equivalente ao nível RAID 5.

- Em caso de falha, processos automatizados distribuem o tráfego para os sites remanescentes.
- Se um servidor falhar, um novo é implantado automaticamente para garantir a continuidade do serviço e o suporte à carga (auto scaling).

2.2.2
Política de backup

Todos os servidores de banco de dados realizam replicação quase em tempo real e são submetidos a backup diário. As cópias de backup são exportadas diariamente, criptografadas e armazenadas de forma segura em um tenant de armazenamento separado, que atua como um cofre. Esses cofres são bloqueados em modo de conformidade, o que significa que ninguém (nem mesmo a AWS) pode excluir os backups durante o período de retenção. O acesso é restrito a administradores da Swile devidamente identificados e autenticados (por exemplo, com autenticação multifator). Os backups são mantidos por um período determinado por restrições legais (GDPR ou outras regulamentações), técnicas, entre outras.

2.2.3
Plano de Continuidade de Negócios e testes

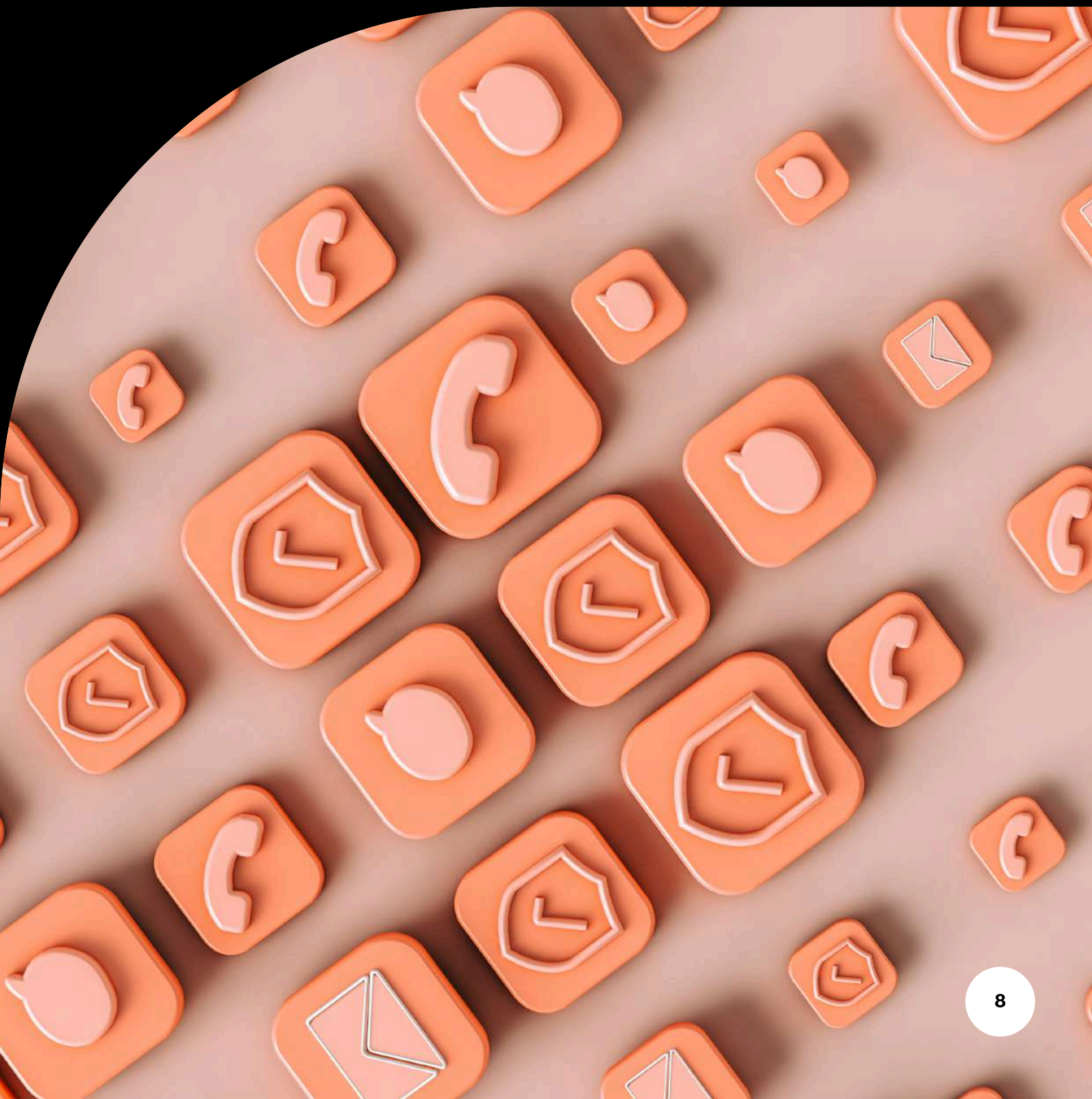
A Swile implementou um plano de continuidade de negócios, baseado em:

- Avaliações de impacto de interrupção para cada processo de negócio sensível;
- Um procedimento de gestão de crises;
- Planos de continuidade operacional que cobrem os produtos da Swile, a TI interna utilizada pelos colaboradores da Swile, escritórios e recursos humanos.

O RPO definido pela Swile é inferior a 24 horas, e o RTO é inferior a 72 horas.

03.

Controles de Segurança



3.1

Controle de Acesso

3.1.1
Política de login e senha dos usuários

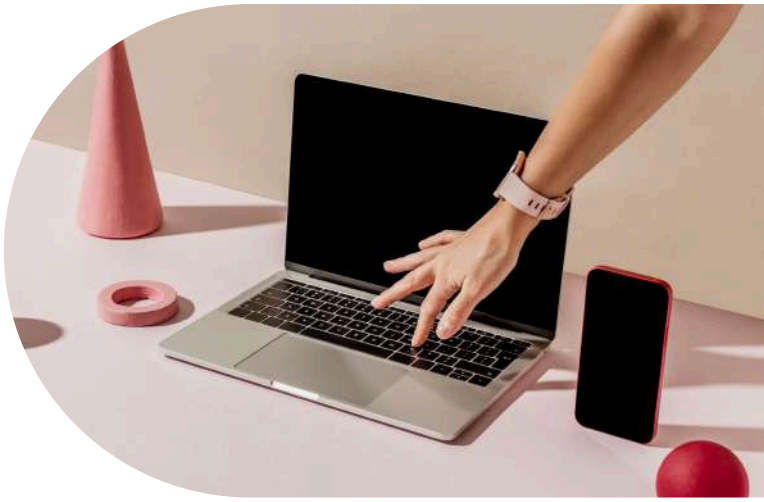
Existem quatro perfis definidos no aplicativo da Swile:

- Beneficiário (colaboradores)
- Gestor (por exemplo, RH, CSR da sua empresa, etc.)
- Operador (Customer Success Manager da Swile, administradores dos sistemas de informação e equipe de suporte ao cliente)
- Afiliado (proprietário de restaurante, varejista)

Os usuários da Swile ativam suas contas por meio de um link de ativação recebido por e-mail. No primeiro acesso ao aplicativo da Swile, é obrigatório definir uma senha segura. A política padrão de senhas da Swile está alinhada aos padrões de segurança. O usuário deve criar uma senha segura contendo, no mínimo, uma letra maiúscula, uma letra minúscula, um número e um símbolo. A reutilização das últimas 10 senhas é proibida.

Um conjunto de proteções está em vigor para prevenir roubo de identidade, como mecanismos de CAPTCHA, sistemas anti–força bruta e análise de comportamento do usuário.

Em conformidade com as regulamentações aplicáveis, um mecanismo de autenticação forte é utilizado para proteger todas as ações sensíveis. Ele consiste no envio de códigos por SMS ao usuário para validação de qualquer operação sensível quando esta não é realizada a partir de um dispositivo confiável (por exemplo, um novo computador ou um novo smartphone).



3.1.2
Política de controle de acesso da Swile

A Swile adota o princípio do menor privilégio para todas as contas de serviço, bem como para seus próprios colaboradores (contas nominativas). Por princípio, os dados permanecem inacessíveis aos colaboradores.

Todo acesso deve ser previamente autorizado pelo gestor direto do colaborador e/ou pela equipe de TI. Por exemplo, os Customer Success Managers têm acesso apenas às regiões pelas quais são diretamente responsáveis. Sempre que possível, as contas são nominativas. As raras contas genéricas estão sujeitas a um processo de exceção e são monitoradas de perto quanto a qualquer anomalia.

A Swile implementou procedimentos de onboarding e offboarding para garantir que cada colaborador tenha os acessos necessários no momento adequado, e que esses acessos sejam bloqueados e suas contas excluídas quando deixam a empresa ou mudam de função. O uso de gerenciamento centralizado de contas e de SSO (Single Sign-On) possibilita a aplicação desses procedimentos. Os acessos são revisados pelo menos uma vez por ano pelos gestores e responsáveis pelos ativos.

A Swile mantém ambientes de desenvolvimento e produção separados. O acesso a cada ambiente é estritamente controlado. O acesso aos servidores da Swile é controlado por meio de chaves assimétricas pessoais, revogáveis e centralizadas em um bastion. A autenticação multifator é obrigatória para qualquer ação administrativa. Por fim, os acessos privilegiados são revisados trimestralmente.

3.2

Segurança de Recursos Humanos

Todas as pessoas que trabalham na Swile possuem uma cláusula de confidencialidade em seus contratos e concordam em cumprir a política de segurança da informação (IT security charter).

Todos os colaboradores são informados sobre as políticas e práticas de segurança da Swile e concordam em cumpri-las como parte do processo inicial de onboarding. Além disso, a Swile realiza treinamentos de conscientização em segurança durante o onboarding e por meio de treinamentos interativos ou exercícios regulares. Como complemento, nossa equipe de segurança organiza periodicamente testes, como campanhas de phishing ou de engenharia social, por exemplo, direcionadas a serviços sensíveis.

Novas contratações para cargos de administradores de sistemas, engenheiros de segurança e outros usuários com acesso privilegiado recebem treinamentos especiais e contínuos (por exemplo: mentoria sobre o OWASP Top 10, competição Swile Secure Code). Esses profissionais também passam por verificações adicionais de antecedentes no momento da contratação (como verificação de antecedentes criminais, conforme a legislação aplicável).

3.3

Proteção de Dados

3.3.1
Criptografia de dados

Os dados são criptografados em trânsito e em repouso, utilizando técnicas de criptografia robustas e confiáveis.

- Em trânsito: todas as trocas são realizadas por meio de HTTPS, SFTP ou outros protocolos criptografados. A comunicação é protegida por TLS 1.2 ou superior, com suporte apenas a cifras fortes. Os certificados dos servidores são contrassinados por uma Autoridade Certificadora reconhecida (Let's Encrypt).
- Em repouso: os dados são criptografados utilizando AES 256 (o gerenciamento e a rotação das chaves são de responsabilidade da Swile: AWS Customer Managed Key).

Para gerenciar fluxos automatizados de dados, a Swile disponibiliza um serviço seguro de troca de arquivos (SFTP com autenticação por chave SSH assimétrica).

As senhas dos usuários da Swile são submetidas a hash e salting antes de serem armazenadas em banco de dados.

Todos os usuários da Swile utilizam um gerenciador de senhas administrado pela empresa, usado para registrar senhas pessoais e para o compartilhamento seguro de segredos entre indivíduos. Os segredos de aplicações e da infraestrutura são armazenados em um cofre digital.

3.3.2
Prevenção de Vazamento de Dados

Os documentos confidenciais da Swile são protegidos por sistemas de Prevenção de Perda de Dados (DLP), que bloqueiam compartilhamentos indevidos ou vazamentos. Todos os repositórios de código-fonte são privados por padrão e não podem ser compartilhados publicamente sem a intervenção da área de Segurança. Esses repositórios também são analisados automaticamente de forma contínua para evitar o armazenamento de segredos.

A Swile contratou um provedor de serviços para coletar informações de inteligência sobre a empresa (CTI) na dark web, deep web e em diversas formas de mídias sociais.

3.4

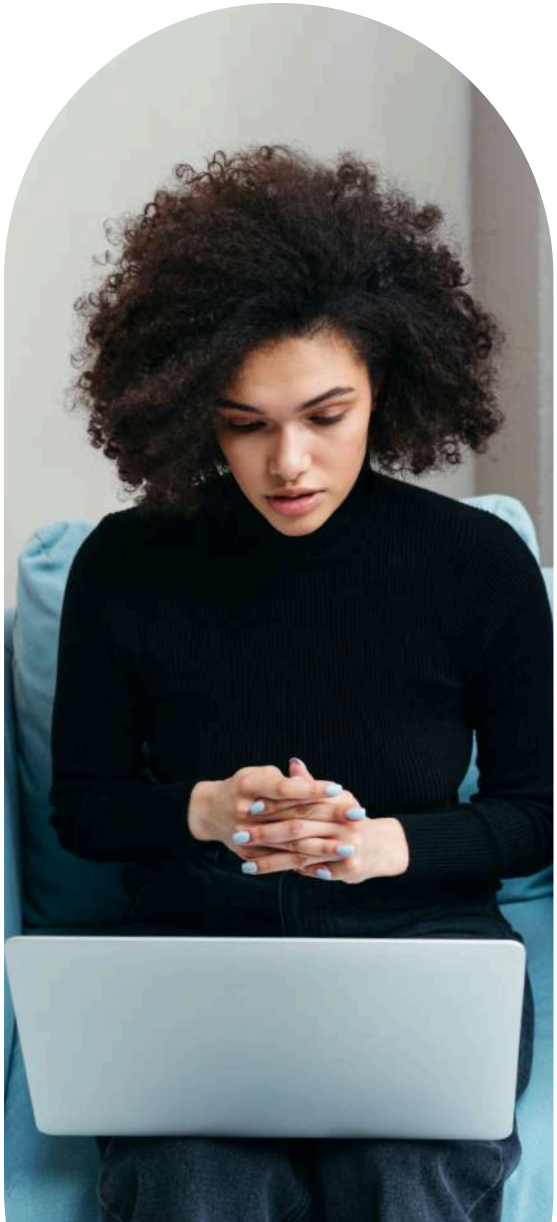
Payment protection

A Swile implementou um sistema de autenticação forte (SCA – Strong Customer Authentication) para limitar fraudes e reforçar a segurança de ações sensíveis realizadas pelos usuários finais nas aplicações da Swile.

A autenticação forte é exigida para ações sensíveis, tais como (lista não exaustiva):

- Visualização de números de cartão;
- Alterações nos dados pessoais do usuário;
- Compras realizadas por meio da plataforma de CSR.

A Swile não processa diretamente informações relacionadas aos cartões dos usuários, pois todos os pagamentos são processados por parceiros certificados PCI-DSS (por exemplo, Stripe, Treezor, entre outros).



3.5

Segurança de Rede

Além do conceito de Security by Design nas aplicações, a Swile protege os fluxos web de entrada em seu sistema de informação por meio de equipamentos e soluções de infraestrutura (por exemplo, WAF, proteção anti-DDoS e anti-robôs).

Os fluxos SFTP que ingressam no sistema de informação da Swile são protegidos por restrições de IP e por particionamento lógico de diretórios.

Os fluxos bancários são seguros por concepção, e a interconexão ocorre por meio de conexões criptografadas com os provedores de serviços bancários.

3.6

Políticas de Gerenciamento de Dispositivos Móveis

A Swile utiliza plataformas de Mobile Device Management (MDM) para controlar e proteger o acesso aos recursos da Swile nos endpoints. A Swile aplica configurações de segurança padronizadas, e todas as estações de trabalho dos colaboradores são:

- Criptografadas em repouso;
- Protegidas por senha (com aplicação de políticas de senha de última geração e expiração de sessão/conta);
- Protegidas por soluções de Endpoint Protection e Endpoint Detection & Response (EDR);
- Gerenciadas por MDM, com a aplicação de um perfil de segurança para hardening;
- Com recursos de geolocalização e limpeza remota (remote wipe);
- Monitoradas centralmente pela equipe de Segurança Operacional.

3.7

Desenvolvimento e Manutenção

Uma abordagem de Security by Design é aplicada e reforçada em todas as etapas da entrega de produtos. A Swile implementou uma política de gestão de mudanças e procedimentos operacionais para garantir a integridade e a disponibilidade de seus serviços.

Existem controles para assegurar que qualquer alteração no código-fonte seja aprovada antes de ser implantada em produção. A aceitação de segurança baseia-se em nosso processo de Peer Review, que exige revisão sistemática pelo responsável do código (code owner), bem como conformidade com regras automatizadas de segurança de código.

Atualmente, operamos:

- Testes estáticos de segurança de aplicações (SAST) integrados ao CI/CD na infraestrutura como código;
- SAST integrados ao CI/CD no código-fonte das aplicações;
- Análise semântica (linters) com regras de segurança uniformes para os desenvolvedores;

Além disso, adotamos a abordagem "Crafting Secure Software" (SDLC), que inclui:

- Um processo de threat modeling e aprimoramento das regras de detecção de vulnerabilidades;
- Documentação, por linguagem, de vulnerabilidades e padrões de correção (Architecture Decision Record – ADR);
- Acompanhamento e orientação (coaching) pela equipe de Segurança.

Atualmente, a Swile não terceiriza atividades de desenvolvimento de código para terceiros.

3.8

Gestão de Vulnerabilidades

A Swile implementou um procedimento de gestão de vulnerabilidades que assegura o monitoramento adequado do sistema de informação e a correção das vulnerabilidades identificadas dentro de prazos definidos.

Os servidores, a configuração da infraestrutura e as aplicações da Swile são regularmente analisados por sistemas de gestão de vulnerabilidades:

- Servidores: por meio de proteção antimalware, varredura de vulnerabilidades e aplicação automática de patches de pacotes do sistema;
- Infraestrutura em nuvem: utilizando serviços de Cloud Security Posture Management (CSPM);
- Configuração da infraestrutura: com SAST e ferramentas de conformidade de segurança;
- Aplicações da Swile: com ferramentas específicas para análise de vulnerabilidades aplicativas (SAST e análise de dependências);
- Estações de trabalho: utilizando soluções de antivírus/antimalware, Endpoint Detection & Response (EDR) e varredura de vulnerabilidades.

Os alertas são tratados pela equipe de Operações de Segurança da Swile.

A Swile é assinante de fontes de informação em Segurança da Informação para receber dados sobre vulnerabilidades novas ou atualizadas, incluindo Security Feeds, associações do setor e serviços de Cyber Threat Intelligence.

Além dos testes ofensivos realizados continuamente de forma interna (campanhas de engenharia social, testes de invasão internos e integração de segurança em projetos), a Swile é submetida a testes de intrusão conduzidos por terceiros em base plurianual.

3.9

Correção de Sistemas (Patching) e Gestão de Configuração

A Swile aplica correções automaticamente em seus servidores de forma diária e realiza, de maneira regular, a reimplantação da infraestrutura de aplicações a partir dos sistemas de gerenciamento de configuração, garantindo que os patches mais recentes sejam aplicados e que a infraestrutura seja restaurada para um estado conhecido e controlado.

A Swile utiliza ferramentas de gerenciamento de configuração (Infrastructure as Code) para automatizar e padronizar esse processo.

A Swile mantém múltiplos ambientes e testa as mudanças em ambientes de staging ativos antes de aplicá-las em ambientes de produção, de acordo com sua política de gestão de mudanças.

A estratégia de correção abaixo é aplicada automaticamente em nossa infraestrutura, de acordo com o nível de severidade da vulnerabilidade e o risco do ativo:

Estratégia de Correção	Crítica	Alta	Média	Baixa
0 - Ativos Críticos de Missão	3 dias*	2 semanas	1 mês	Melhor esforço
1 - Ativos Essenciais de Missão	2 semanas	1 mês	Melhor esforço	Melhor esforço
2 - Ativos Secundários de Missão	1 mês	Melhor esforço	Melhor esforço	Melhor esforço

*Prazos indicativos, sujeitos a validação operacionais e de segurança.

3.10

Monitoramento e Registro de Eventos

Para fins de monitoramento técnico, manutenção e suporte, a Swile utiliza ferramentas integradas para garantir o correto funcionamento de aplicações, processos, contêineres e servidores, incluindo, entre outros:

- Monitoramento de processos;
- Monitoramento de recursos (CPU, RAM, espaço em disco);
- Monitoramento de disponibilidade e health checks das aplicações;
- Monitoramento funcional;
- Monitoramento específico de bancos de dados;
- Monitoramento de desempenho de aplicações (APM);
- Monitoramento de erros e códigos de retorno;
- Monitoramento de segurança das aplicações;
- Monitoramento do comportamento dos usuários.

Todos os sistemas utilizados na prestação dos serviços da Swile, incluindo servidores, contêineres, firewalls, reverse-proxies, componentes de rede, componentes de segurança e sistemas operacionais, registram informações em um repositório centralizado de logs, permitindo a análise de eventos de segurança e a adoção de respostas adequadas.

A Swile possui alertas automatizados sobre esses logs. Os dados de log são automaticamente enriquecidos por fontes internas e externas de inteligência de ameaças para detecção avançada. Alertas e incidentes são tratados pela equipe de segurança.

Os logs são armazenados em um log sink e posteriormente arquivados em um local de armazenamento seguro e imutável, em conformidade com a estratégia de backup. As equipes de segurança podem reimportar esses logs em ferramentas de análise para fins de investigação e evidência.

3.11

Detecção e Prevenção de Intrusões

A Swile protege ativamente suas aplicações contra ataques por meio de medidas como técnicas de particionamento de rede, firewalls de rede e de aplicações (WAF) e dispositivos IDS/IPS. A proteção anti-DDoS (camadas OSI 3 e 4) é gerenciada por meio do provedor de hospedagem AWS.

A Swile monitora aplicações, sistemas, usuários, servidores e estações de trabalho em toda a sua infraestrutura utilizando sistemas de detecção de intrusão baseados em host e em contêineres, soluções de proteção de endpoint e ferramentas de análise de comportamento de usuários. Os alertas são monitorados pela equipe interna de Segurança Operacional.

Além disso, a Swile pode analisar dados técnicos e totalmente anônimos coletados pelos navegadores web dos usuários (por exemplo, tipo de dispositivo, resolução de tela, fuso horário, versão do sistema operacional, tipo e versão do navegador, fontes do sistema, plug-ins de navegador instalados, tipos MIME habilitados etc.) para fins de segurança, incluindo a prevenção de autenticações fraudulentas e a garantia do correto funcionamento dos serviços da Swile.

As APIs e o painel (dashboard) da Swile utilizam controles de acesso rigorosos baseados em perfis de usuário. Requisições web e chamadas de API não autorizadas são registradas em log.

3.12

Gestão de Incidentes de Segurança da Informação

A Swile possui políticas e procedimentos documentados e regularmente auditados para a gestão de incidentes e crises de segurança, incluindo um plano de resposta a incidentes.

3.13

Segurança Física e Ambiental

Toda a infraestrutura da Swile é hospedada em datacenters e servidores gerenciados e controlados pelo provedor de nuvem Amazon Web Services. Os colaboradores da Swile não possuem acesso físico a esses datacenters.

Detalhes sobre as práticas e controles de segurança aplicáveis a essas instalações podem ser consultados no site da AWS.

O acesso aos escritórios da Swile é controlado por segurança 24 horas. Existe um sistema de controle de acesso por crachás, além de videomonitoramento em pontos críticos.

3.14

Bloqueio de Acesso de Terceiros

Os serviços da Swile não foram projetados para incluir backdoors ou funcionalidades semelhantes que permitam ao governo ou a quaisquer terceiros acessar os Dados dos Clientes. A Swile não fornece voluntariamente a governos ou a terceiros chaves de criptografia, nem qualquer outro meio de quebrar sua criptografia ou, de forma geral, qualquer tipo de acesso aos seus dados.

04.

Compliance Regulatória, LGPD e Banco Central do Brasil (BACEN)

A Swile está comprometida com o cumprimento integral da legislação e das regulamentações aplicáveis à proteção de dados pessoais, à segurança da informação e à estabilidade do sistema financeiro, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) e as normas emitidas pelo Banco Central do Brasil (BACEN), quando aplicáveis ao seu modelo de atuação.

Os princípios da LGPD — como finalidade, adequação, necessidade, segurança, prevenção e responsabilização — são incorporados aos processos internos, às políticas corporativas e às práticas de segurança da Swile ao longo de todo o ciclo de vida dos dados pessoais.

No contexto regulatório do BACEN, a Swile adota práticas de governança, gestão de riscos, segurança cibernética e continuidade de negócios alinhadas às resoluções e circulares vigentes, assegurando:

- Estrutura formal de governança e responsabilidades definidas;
- Avaliação contínua de riscos operacionais, tecnológicos e de segurança da informação;
- Mecanismos de prevenção, detecção e resposta a incidentes;
- Processos de auditoria, monitoramento e reporte, quando exigidos.

A Swile realiza revisões periódicas de seus controles, políticas e processos, considerando atualizações regulatórias, orientações das autoridades competentes e melhores práticas de mercado, garantindo a evolução contínua do seu nível de conformidade e de confiança digital.

05.

Contatos

A equipe de Segurança da Swile pode ser contatada pelo e-mail:
security@swile.co

A política de divulgação responsável
(Responsible Disclosure Policy) pode ser encontrada em:
https://swile.co/.well-known/security.txt