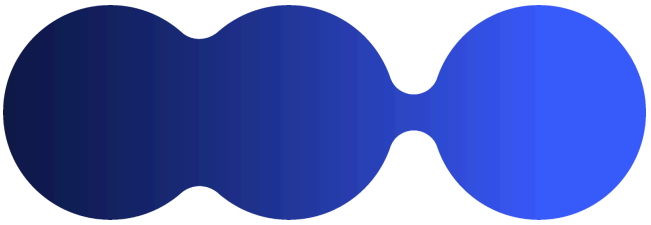


PrivSecOps

Security Overview

Versão Português

pipefy Security Overview

Sumário

DATACENTER E SEGURANÇA DE REDE DO PIPEFY

Segurança física

NOME	DETALHES
Instalações	A infraestrutura física dos provedores de serviços do Pipefy é hospedada e gerenciada em data centers seguros da Oracle e utiliza a tecnologia Oracle Cloud Infrastructure (OCI). A Oracle gerencia riscos e passa por avaliações recorrentes para garantir a conformidade de acordo com os padrões do setor. As operações de data center da Oracle foram credenciadas em: • ISO 27001 • ISO 27701 • ISO 27018 • ISO 42001 • SOC 1 e SOC 2/SSAE 16/ISAE 3402 (anteriormente SAS 70 Tipo II) • PCI Nível 1 • FISMA Moderado • Lei Sarbanes-Oxley (SOX) Caso o cliente necessite utilizar uma solução multicloud, o Pipefy analisará o caso e disponibilizará outros provedores de nuvem, com a mesma qualidade da AWS.
Segurança local	Pipefy utiliza datacenters certificados ISO 27001 e FISMA gerenciados pela Oracle. Os data centers da OCI estão alojados em instalações indefinidas, e as instalações críticas têm amplos recuos e bermas de controle de perímetro de nível militar, bem como outras proteções de limites naturais. O acesso físico é estritamente controlado tanto no perímetro como nos pontos de entrada do edifício por pessoal de segurança profissional, utilizando vigilância por vídeo, sistemas de detecção de intrusão de última geração e outros meios eletrônicos. A equipe autorizada deve passar pela autenticação de dois fatores pelo menos três vezes para acessar os andares do data center. Todos os visitantes e contratados são obrigados a apresentar identificação e são registrados e continuamente acompanhados por pessoal autorizado.
Localização	Os datacenters dos provedores de serviços do Pipefy estão localizados nos Estados Unidos. Se o cliente quiser solicitar um único locatário, vários locais em todo o mundo estarão disponíveis usando diferentes soluções em nuvem.

Segurança de rede

NOME	DETALHES
Equipe de resposta de segurança	Nossa equipe de resposta de segurança está de plantão para responder a alertas e eventos de segurança e pode ser contatada em segurança@pipefy.com.
Proteção	A infraestrutura e o gerenciamento de todos os firewalls são fornecidos pelo nosso provedor de serviços Oracle OCI. Firewalls são utilizados para restringir o acesso a sistemas de redes externas e entre sistemas internos. Por padrão, todo o acesso é negado e apenas portas e protocolos explicitamente permitidos são permitidos com base nas necessidades do negócio. Cada sistema é atribuído a um grupo de segurança de firewall com base na função do sistema. Os grupos de segurança restringem o acesso às portas e protocolos necessários para a função específica de um sistema, a fim de mitigar riscos. Os firewalls baseados em host também oferecem a capacidade de limitar ainda mais as conexões de entrada e saída conforme necessário.
Gerenciamento de vulnerabilidades	Nossos firewalls gerenciados pelo provedor de serviços evitam a falsificação de IP, MAC e ARP na rede e entre hosts virtuais para garantir que a falsificação não seja possível. A detecção de pacotes é evitada pela infraestrutura, incluindo o hipervisor, que não entregará tráfego a uma interface à qual não está endereçado. Nosso provedor de serviços utiliza isolamento de aplicativos, restrições de sistema operacional e conexões criptografadas para garantir ainda mais a mitigação de riscos em todos os níveis. A varredura de portas é proibida e cada instância relatada é investigada pelo nosso fornecedor de infraestrutura. Quando as varreduras de portas são detectadas, elas são interrompidas e o acesso é bloqueado.
Testes de penetração e monitoramento de vulnerabilidade	O Pipefy possui uma equipe especializada responsável por pentests internos e avaliações de vulnerabilidades. Esses testes são realizados pelo menos uma vez trimestralmente. Os testes de segurança de nossos serviços por terceiros podem ser realizados por empresas de consultoria de segurança independentes e respeitáveis, contratadas pelo cliente. As possíveis descobertas de cada avaliação seriam revisadas com os avaliadores, classificadas em termos de risco e atribuídas à equipe responsável para resolvê-las sob um SLA.

	Esses testes serão feitos pelo cliente e todos os encargos envolvidos são de responsabilidade do cliente.
Evento e resposta a incidentes de segurança	No caso de um incidente de segurança, nossos engenheiros são chamados para coletar registros extensos de sistemas host críticos e analisá-los para responder ao incidente da maneira mais adequada possível. Coletar e analisar informações de log é fundamental para solucionar problemas e investigar problemas. Nosso provedor de serviços nos permite analisar três tipos principais de logs: logs sistêmicas, de aplicativo e de API. Podem existir responsabilidades compartilhadas entre o Pipefy e nossos provedores de nuvem, e essas responsabilidades serão de responsabilidade da equipe de segurança do Pipefy.
Mitigação de DDoS	A infraestrutura do nosso provedor de serviços fornece técnicas de mitigação de DDoS, incluindo cookies TCP Syn e limitação de taxa de conexão, além de manter múltiplas conexões de backbone e capacidade de largura de banda interna que excede a largura de banda fornecida pela operadora de Internet. Trabalhamos em estreita colaboração com nossos fornecedores para responder rapidamente a eventos e ativar controles avançados de mitigação de DDoS quando necessário.
Acesso Lógico	O acesso à Rede de Produção Pipefy é restrito por uma necessidade explícita de conhecimento. Ele utiliza privilégios mínimos, é frequentemente auditado e controlado de perto por nossa equipe de engenharia. Os funcionários que acessam a Rede de Produção do Pipefy são obrigados a usar múltiplos fatores de autenticação.

Criptografia e autenticação

POLÍTICA	DETALHES
Criptografia na transferência	Toda a comunicação interna e externa é feita através de uma conexão segura com TLS 1.2 ou superior.
Criptografia na transferência – E-mails	Todos os emails são enviados pelo Sendgrid através de uma conexão TLS segura.

Criptografia em repouso e em backup	Os dados em repouso são criptografados por meio do algoritmo AES-256. O backup é feito através de snapshot, também com criptografia AES-256.

Disponibilidade e Continuidade

POLÍTICA	DETALHES
Tempo de atividade	O Pipefy foi construído pensando na alta disponibilidade e nossa equipe de engenharia monitora continuamente para garantir sua disponibilidade. A disponibilidade nos últimos 2 anos é de 99,9% ou superior, podendo ser consultada no nosso site em: status.pipefy.com.
Redundância	O clustering do provedor de serviços Pipefy e as redundâncias de rede eliminam pontos únicos de falha.
Recuperação de desastres	A plataforma do nosso provedor de serviços restaura automaticamente os aplicativos e bancos de dados dos clientes em caso de interrupção. A plataforma do provedor foi projetada para implantar aplicativos dinamicamente em sua nuvem, monitorar falhas e recuperar componentes da plataforma com falha, incluindo aplicativos e bancos de dados de clientes.

pipefy Security Overview

SEGURANÇA DA APLICAÇÃO

Desenvolvimento Seguro (SDLC)

POLÍTICA	DETALHES
Controles de segurança da estrutura Ruby on Rails	Utilizamos controles de segurança da estrutura Ruby on Rails para limitar a exposição às 10 principais falhas de segurança do OWASP. Isso inclui controles inerentes que reduzem nossa exposição a Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) e SQL Injection (SQLi), entre outros.
Controle de qualidade	Nosso departamento de controle de qualidade analisa e testa nossa base de código. Engenheiros de aplicação dedicados na equipe identificam, testam e fazem a triagem de vulnerabilidades de segurança no código.
Ambientes Separados	Os ambientes de teste e preparação são separados do ambiente de produção. Nenhum dado real do cliente é usado nos ambientes de desenvolvimento ou teste.

Vulnerabilidades de aplicativos

POLÍTICA	DETALHES
Análise de código estático	Nossos repositórios de código-fonte são continuamente verificados em busca de problemas de segurança por meio de nossas ferramentas integradas de análise estática.

RECURSOS DE SEGURANÇA DO PRODUTO

Desenvolvimento Seguro (SDLC)

RECURSO	DETALHES
Opções de autenticação	Pipefy suporta login, SSO e autenticação Google.
Logon único (SSO)	O login único (SSO) permite autenticar usuários em seus próprios sistemas sem exigir que eles insiram credenciais de login adicionais para acesso ao Pipefy.
Armazenamento seguro de credenciais	O Pipefy segue as melhores práticas de armazenamento seguro de credenciais, nunca armazenando senhas em formato legível por humanos.
Segurança e autenticação de API	A API do Pipefy é somente SSL e você deve ser um usuário verificado para fazer solicitações de API. Você pode autorizar na API usando o token da API.

Recursos adicionais de segurança do produto

POLÍTICA	DETALHES
Privilégios e funções de acesso	O acesso aos dados da sua conta Pipefy é regido por direitos de acesso e pode ser configurado para definir privilégios de acesso. O Pipefy possui vários níveis de permissão para usuários da organização (membro e administrador) e do pipe (somente formulário inicial, membro e administrador). Mais detalhes podem ser vistos aqui.
Segurança de Transmissão	Todas as comunicações com os servidores dos provedores de serviços do Pipefy são criptografadas usando HTTPS padrão do setor. Isso garante que todo o tráfego entre você e o Pipefy esteja seguro durante o trânsito.

RECURSOS DE INTELIGÊNCIA ARTIFICIAL

Sistema de gestão de Inteligência Artificial

DESTAQUE	DETALHES
Objetivos	Os objetivos estratégicos do sistema de gestão de Inteligência Artificial (SGIA) são aqueles que a Pipefy pretende atingir de acordo com sua visão corporativa de governança e uso responsável de IA, estando alinhados ao Plano Estratégico Corporativo e às diretrizes da ISO/IEC 42001. Entre esses objetivos estão: • Promover o cumprimento das leis, normas e regulamentos aplicáveis ao uso de inteligência artificial, assegurando conformidade ética, técnica e legal; • Garantir transparência, confiabilidade e segurança no desenvolvimento e operação de soluções de IA integradas à Plataforma Pipefy; • Mitigar riscos associados ao uso de IA, por meio de processos contínuos de avaliação, monitoramento e melhoria de controles técnicos e de governança; • Assegurar a proteção e privacidade dos dados dos clientes, reforçando práticas de não retenção, descarte seguro e uso limitado das informações processadas; • Aumentar a conscientização e capacitação interna sobre uso responsável da IA, fortalecendo a cultura organizacional em torno da ética e da inovação confiável.
Produtos	• Agente IA: O Agente IA do Pipefy é projetado para atuar de forma autônoma, assumindo tarefas e processos do início ao fim sem depender de intervenção humana. Ele pode, por exemplo, classificar e organizar demandas recebidas, movimentar cards entre fases, solicitar informações adicionais ou até acionar fluxos de automação integrados a outros sistemas. A grande vantagem do Agente IA é que ele não apenas auxilia, mas realmente executa o trabalho por conta própria • Copiloto IA: Essa IA funciona como um parceiro inteligente que acompanha o usuário em suas atividades diárias dentro do Pipefy. Em vez de tomar decisões sozinho, ele oferece suporte para acelerar tarefas e reduzir erros, sugerindo conteúdos, preenchendo dados automaticamente, resumindo informações ou até gerando respostas personalizadas em diferentes contextos. O foco do Copiloto é aumentar a produtividade do usuário, permitindo que cada pessoa se

concentre no que exige análise humana, enquanto a IA cuidar das partes repetitivas ou operacionais

- Assistente IA: O Assistente IA é a interface conversacional que torna a interação com os processos mais intuitiva e acessível. Ele permite que usuários façam perguntas em linguagem natural, solicitem ações específicas ou peçam resumos diretamente dentro da plataforma. Dessa forma, mesmo quem não conhece a fundo a estrutura de um pipe pode navegar, executar tarefas e obter insights rapidamente, apenas dialogando com o assistente. É uma forma de transformar o Pipefy em um ambiente mais simples, inteligente e fácil de usar para todos os níveis da organização.

Conscientização sobre Inteligência Artificial

METODOLOGIA	DETALHES
Políticas	O Pipefy desenvolveu um conjunto abrangente de políticas como nossa Política de Segurança da Informação e nossa Política de Privacidade de Dados Pessoais, que englobam também tópicos de IA. Ademais, desenvolvemos também uma Política de Governança de Inteligência direcionada para temas éticos e sociais envolvendo essa tecnologia. Essas políticas são compartilhadas e disponibilizadas a todos os funcionários e prestadores de serviços com acesso aos ativos de informação do Pipefy. Os Relatórios de Auditoria não são compartilhados externamente, apenas os resultados e o nível de maturidade do ambiente Pipefy.
Treinamento	Todos os novos funcionários participam de um Treinamento de Conscientização sobre IA durante o processo de integração, e todos os funcionários realizam este treinamento uma vez por ano. Nos treinamentos anuais, a companhia foca em conscientizar sobre os principais tópicos relacionados à Inteligência Artificial, incluindo o entendimento de Modelos de Linguagem de Grande Escala (LLMs), o funcionamento de ferramentas como o ChatGPT e outros assistentes de IA, boas práticas de uso seguro e ético da IA, riscos e limitações de sistemas de IA, privacidade e segurança de dados no contexto de IA, e como a IA pode impactar processos e decisões na empresa. O Pipefy também disponibiliza cursos para elevar as habilidades dos clientes/ usuários sobre a Inteligência Artificial do Pipefy. Através da Pipefy Academy é possível aproveitar, ao máximo, os recursos do Pipefy e viabilizar a otimização dos processos.

Canal de relatos e comunicação	No Pipefy, estamos comprometidos com o uso responsável da Inteligência Artificial e com a proteção de seus dados. Trabalhamos para implementar as melhores práticas e medidas que garantam a segurança, ética e conformidade no uso de IA, sempre em alinhamento com os requisitos da ISO 42001 Nosso objetivo é manter um alto nível de maturidade em nossas práticas de IA, prevenindo riscos e monitorando possíveis desvios de IA, para que todas as decisões automatizadas sejam justas, seguras e transparentes. Você pode obter mais informações sobre nossas políticas de ética e compliance relacionadas à IA e desvios de IA no nosso Canal de Relatos: https://www.pipefy.com/pt-br/etica-e-compliance/ Para qualquer dúvida e solicitação, entre em contato com nossa Central de Ajuda https://help.pipefy.com/

METODOLOGIAS DE SEGURANÇA

Sistema de gerenciamento de segurança da informação

DESTAQUE	DETALHES
Objetivos	Os objetivos estratégicos de segurança da informação (objetivos estratégicos do SGSI) são aqueles que o Pipefy pretende atingir de acordo com uma visão corporativa de segurança da informação e que estão alinhados com os objetivos mencionados em seu Plano Estratégico Corporativo, entre os quais estão: • Promover o cumprimento das leis, normas e regulamentos relativos ao negócio nos seus aspectos relacionados à Segurança da Informação; • Melhorar continuamente os controles de segurança e maturidade da Plataforma Pipefy para mitigar riscos; • Aumentar o conhecimento e a consciência interna sobre a necessidade de Segurança da Informação para o negócio.

Conscientização sobre Segurança da Informação

METODOLOGIA	DETALHES
Políticas	O Pipefy desenvolveu um conjunto abrangente de políticas de segurança que abrangem diversos tópicos. Essas políticas são compartilhadas e disponibilizadas a todos os funcionários e prestadores de serviços com acesso aos ativos de informação do Pipefy. Os Relatórios de Auditoria não são compartilhados externamente, apenas os resultados e o nível de maturidade do ambiente Pipefy.
Treinamento	Todos os novos funcionários participam de um Treinamento de Conscientização sobre Segurança, assim como todos os funcionários realizam o mesmo treinamento uma vez por ano. Além disso, todos os colaboradores participam de treinamentos sobre Privacidade de Dados, GDPR e LGPD. Todos os membros da equipe de Engenharia também participam uma vez por ano (exceto o Treinamento de Conscientização em Segurança) de um Treinamento de Desenvolvimento Seguro baseado no OWASP TOP 10 e SANS 25. A Conscientização em Segurança também faz parte da rotina do Pipefy, pois as atualizações são compartilhadas entre todas as equipes via e-mail, postagens em blogs e em apresentações durante eventos internos.
Medidas de privacidade	No Pipefy estamos cientes da sua privacidade e dos seus direitos e trabalhamos para entregar a você as melhores práticas e medidas para manter seus dados seguros. Estamos de acordo com os requisitos da LGPD e GDPR. E estamos trabalhando incansavelmente, todos os dias, para manter um alto nível de maturidade em nossas medidas de segurança. Você pode ver mais informações sobre Privacidade, no Pipefy em: • Página de privacidade mundial: https://www.pipefy.com/privacy-policy/ • Página de privacidade brasileira: https://www.pipefy.com/pt-br/politica-de-privacidade/ Para qualquer dúvida e solicitação, entre em contato pelo nosso e-mail: privacidade@pipefy.com. E-mail do nosso DPO: dpo@pipefy.com.

Verificação de funcionários

METODOLOGIA	DETALHES
Verificação em segundo plano	O Pipefy realiza verificações de antecedentes de todos os novos funcionários de acordo com as leis locais. A verificação de antecedentes inclui verificação criminal, educacional e de emprego.
Acordos de Confidencialidade	Todas as novas contratações são avaliadas durante o processo de contratação e obrigadas a assinar acordos de não divulgação e confidencialidade de acordo com as leis locais.

CERTIFICAÇÕES E DOCUMENTAÇÕES ADICIONAIS

CERTIFICAÇÃO	DETALHES
ISO 42001	O padrão ISO/IEC 42001 é a primeira norma internacional dedicada à gestão responsável da Inteligência Artificial (IA). Ele estabelece uma estrutura de melhores práticas para Sistemas de Gestão de Inteligência Artificial (SGIA), garantindo que organizações adotem controles técnicos, éticos e de governança para desenvolver, implantar e operar sistemas de IA de forma segura, confiável e transparente.
ISO 27001	O padrão ISO 27001 é a estrutura de melhores práticas reconhecida internacionalmente para um Sistema de Gestão de Segurança da Informação (SGSI).

ISO 27701

ISO 27701 é o padrão internacional de privacidade que fornece uma estrutura para gerenciamento de privacidade de dados. É uma extensão de privacidade de dados da ISO 27001.

ISO 27018

ISO 27018 é o código de prática para proteger informações de identificação pessoal (PII) em serviços de computação em nuvem.

SOC 1 e 2 tipo 2

SOC 1 e 2 são relatórios atualizados regularmente que se concentram em controles relacionados a controles financeiros, segurança, disponibilidade e confidencialidade de um serviço em nuvem. O Pipefy pode compartilhar relatórios SOC 1 e 2, através de um acordo de não divulgação (NDA) assinado.

Software qualificado AWS

Nosso fornecedor AWS analisa nossa infraestrutura e segurança de aplicativos por meio da Revisão Técnica Fundamental (FTR). Esse processo garante que nossa implementação e uso da nuvem foram validados pela AWS por sua proficiência técnica e referências de clientes associadas.

Questionário da Iniciativa de Avaliações de Consenso (CAIQ)

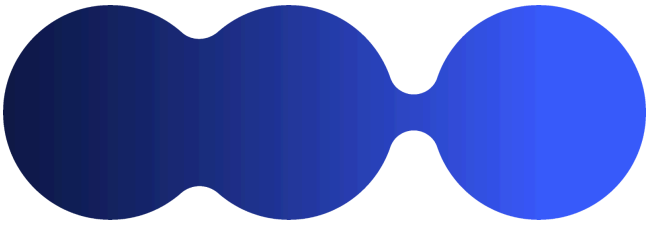
O questionário CAIQ fornece uma maneira aceita pelo setor de documentar quais controles de segurança existem nos serviços em nuvem. Isto aumenta a transparência do controle de segurança para clientes atuais e potenciais, que podem então determinar se nossos serviços são seguros o suficiente para seus propósitos.

O questionário preenchido pode ser obtido por meio de um acordo de não divulgação (NDA) assinado.

HISTÓRICO DE REVISÃO

Versão	Data	Time responsável	Descrição
1.0	22/05/2022	PrivSecOps	Criação do Documento
2.0	20/05/2023	PrivSecOps	Revisão anual; Adição de certificações do escopo.
3.0	17/06/2024	PrivSecOps	Revisão Anual; Ajuste de Template.
4.0	28/03/2025	PrivSecOps	Revisão Anual.
5.0	01/09/2025	PrivSecOps	Revisão com adição de certificações do escopo.

ENGLISH VERSION OF THE PROCEDURE



PrivSecOps

Security Overview

English version

Public Information

Summary

pipefy Security Overview

PIPEFY DATACENTER AND NETWORK SECURITY

Physical security

NAME	DETAILS
Facilities	The physical infrastructure of Pipefy service providers is hosted and managed in secure Oracle data centers and uses Oracle Cloud Infrastructure (OCI) technology. Oracle manages risk and undergoes recurring assessments to ensure compliance with industry standards. Oracle's data center operations have been accredited in: • ISO 27001 • ISO 27701 • ISO 27018 • ISO 42001 • SOC 1 and SOC 2/SSAE 16/ISAE 3402 (formerly SAS 70 Type II) • PCI Level 1 • FISMA Moderate • Lei Sarbanes-Oxley (SOX) If the customer needs to use a solution multicloud, Pipefy will analyze the case and make other cloud providers available, with the same quality as AWS.
Local security	Pipefy uses ISO 27001 and FISMA certified data centers managed by Oracle. OCI data centers are housed in nondescript facilities, and critical facilities have extensive military-grade perimeter control setbacks and berms, as well as other natural boundary protections. Physical access is strictly controlled at both the perimeter and building entry points by professional security personnel utilizing video surveillance, state-of-the-art intrusion detection systems and other electronic means. Authorized staff must undergo two-factor authentication at least three times to access data center floors. All visitors and contractors are required to present identification and are registered and continuously monitored by authorized personnel.
Location	Pipefy service providers' data centers are located in the United States. If the customer wants to request a single tenant, multiple locations across the world are available using different cloud solutions.

Network security

NAME	DETAILS
Security Response Team	Our security response team is on call to respond to security alerts and events and can be reached at segurança@pipefy.com.
Protection	Infrastructure and management for all firewalls is provided by our service provider Oracle OCI. Firewalls are used to restrict access to external network systems and between internal systems. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business needs. Each system is assigned a firewall security group based on the system's role. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.
Vulnerability Management	Our service provider-managed firewalls prevent IP, MAC, and ARP spoofing within the network and between virtual hosts to ensure that spoofing is not possible. Packet sniffing is prevented by the infrastructure, including the hypervisor, which will not deliver traffic to an interface to which it is not addressed. Our service provider utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk mitigation at all levels. Port scanning is prohibited and each reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.
Penetration Testing and Vulnerability Monitoring	Pipefy has a specialized team responsible for pentests internal and vulnerability assessments. These tests are performed at least once quarterly. Third-party security testing of our services may be performed by reputable, independent security consulting firms engaged by the customer. Potential findings from each assessment would be reviewed with assessors, classified in terms of risk, and assigned to the responsible team to resolve them under an SLA. These tests will be carried out by the customer and all charges involved are the customer's responsibility.

Event and security incident response	In the event of a security incident, our engineers are called upon to collect extensive logs from critical host systems and analyze them to respond to the incident as appropriately as possible. Collecting and analyzing log information is critical for troubleshooting and investigating problems. Our service provider allows us to analyze three main types of logs: systemic, application, and API logs. There may be shared responsibilities between Pipefy and our cloud providers, and these responsibilities will be the responsibility of the Pipefy security team.
DDoS Mitigation	Our service provider's infrastructure provides DDoS mitigation techniques, including TCP Syn cookies and connection rate limiting, as well as maintaining multiple backbone connections and internal bandwidth capacity that exceeds the bandwidth provided by the Internet operator. We work closely with our vendors to quickly respond to events and activate advanced DDoS mitigation controls when necessary.
Logical Access	Access to the Pipefy Production Network is restricted by an explicit need to know. It uses least privileges, is often audited and closely controlled by our engineering team. Employees accessing the Pipefy Production Network are required to use multiple authentication factors.

Encryption and authentication

POLICY	DETAILS
Encryption on transfer	All internal and external communication is done through a secure connection with TLS 1.2 or higher.
Encryption in transfer – Emails	All emails are sent by Sendgrid over a secure TLS connection.
Encryption at rest and in backup	Data at rest is encrypted using the AES-256 algorithm. Backup is done via snapshot, also with AES-256 encryption.

Availability and Continuity

POLICY	DETAILS
Uptime	Pipefy was built with high availability in mind and our engineering team continuously monitors it to ensure its availability. Availability in the last 2 years is 99.9% or higher, and can be found on our website at: status.pipefy.com.
Redundancy	Pipefy service provider clustering and network redundancies eliminate single points of failure.
Disaster recovery	Our service provider platform automatically restores customers' applications and databases in the event of an outage. The provider's platform is designed to dynamically deploy applications to your cloud, monitor failures, and recover failed platform components, including applications and customer databases.

APPLICATION SECURITY

Safe Development (SDLC)

POLICY	DETAILS
Ruby on Rails framework security controls	We use security controls from the Ruby on Rails framework to limit exposure to the OWASP Top 10 Security Flaws. This includes inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
Quality control	Our QA department reviews and tests our code base. Dedicated application engineers on the team identify, test, and triage security vulnerabilities in code.
Separate Environments	Test and staging environments are separate from the production environment. No actual customer data is used in the development or testing environments.

Application vulnerabilities

POLICY	DETAILS
Static code analysis	Our source code repositories are continually scanned for security issues through our built-in static analysis tools.

PRODUCT SAFETY FEATURES

Safe Development (SDLC)

RESOURCE	DETAILS
Authentication Options	Pipefy supports Google login, SSO and authentication.
Single sign-on (SSO)	Single sign-on (SSO) allows you to authenticate users to your own systems without requiring them to enter additional login credentials to access Pipefy.
Secure Credential Storage	Pipefy follows best practices for secure credential storage, never storing passwords in a human-readable format.
API security and authentication	The Pipefy API is SSL-only and you must be a verified user to make API requests. You can authorize on API using API token.

Additional product safety features

POLICY	DETAILS
Access privileges and roles	Access to your Pipefy account data is governed by access rights and can be configured to define access privileges. Pipefy has several permission levels for organization (member and admin) and pipe users (initial form, member and admin only).

	More details can be seen here.
Transmission Security	All communications with Pipefy service providers' servers are encrypted using industry-standard HTTPS. This ensures that all traffic between you and Pipefy is secure in transit.

ARTIFICIAL INTELLIGENCE RESOURCES

Artificial Intelligence Management System

POLICY	DETAILS
Goals	Strategic objectives of the Artificial Intelligence Management System (AIMS) are those that Pipefy intends to achieve in line with its corporate vision of governance and the responsible use of AI, aligned with the Corporate Strategic Plan and the guidelines of ISO/IEC 42001. Among these objectives are: • Promote compliance with laws, standards, and regulations applicable to the use of artificial intelligence, ensuring ethical, technical, and legal conformity; • Ensure transparency, reliability, and security in the development and operation of AI solutions integrated into the Pipefy Platform; • Mitigate risks associated with the use of AI through continuous processes of assessment, monitoring, and improvement of technical and governance controls; • Ensure the protection and privacy of customer data, reinforcing practices of non-retention, secure disposal, and limited use of processed information; • Increase internal awareness and training on the responsible use of AI, strengthening the organizational culture around ethics and trustworthy innovation.
Products	• AI Agent: The Pipefy AI Agent is designed to operate autonomously, handling tasks and processes from start to finish without relying on human intervention. For example, it can classify and organize incoming requests, move cards between phases, request additional information, or even

trigger automation flows integrated with other systems. The key advantage of the AI Agent is that it doesn't just assist—it actually executes the work on its own.

- AI Copilot: This AI works as an intelligent partner that accompanies the user in their daily activities within Pipefy. Instead of making decisions independently, it provides support to speed up tasks and reduce errors by suggesting content, auto-filling data, summarizing information, or even generating personalized responses in different contexts. The Copilot's focus is on boosting user productivity, allowing each person to concentrate on what requires human analysis, while AI takes care of repetitive or operational tasks.
- AI Assistant: The AI Assistant is the conversational interface that makes interaction with processes more intuitive and accessible. It allows users to ask questions in natural language, request specific actions, or ask for summaries directly within the platform. This way, even those unfamiliar with the structure of a pipe can navigate, complete tasks, and quickly gain insights simply by dialoguing with the assistant. It's a way of transforming Pipefy into a smarter, simpler, and more user-friendly environment for all levels of the organization.

Artificial Intelligence Awareness

METHODOLOGY	DETAILS
Policies	Pipefy has developed a comprehensive set of policies, such as our POL.01 Information Security Policy and our POL.08 Personal Data Privacy Policy, which also cover AI-related topics. In addition, we have developed an Artificial Intelligence Governance Policy focused on ethical and social issues involving this technology. These policies are shared and made available to all employees and service providers with access to Pipefy's information assets. Audit Reports are not shared externally; only the results and the maturity level of the Pipefy environment are disclosed
Training	All new employees participate in an AI Awareness Training during the onboarding process, and all employees complete this training once a year. In the annual trainings, the company focuses on raising awareness about key topics related to Artificial Intelligence, including the understanding of Large Language Models (LLMs), how tools like ChatGPT and other AI assistants work, best practices for safe and ethical use of AI, risks and

	limitations of AI systems, data privacy and security in the context of AI, and how AI can impact processes and decision-making within the company.
Reporting and communication channel	At Pipefy, we are committed to the responsible use of Artificial Intelligence and the protection of your data. We work to implement best practices and measures that ensure security, ethics, and compliance in the use of AI, always in alignment with the requirements of ISO 42001. Our goal is to maintain a high level of maturity in our AI practices, preventing risks and monitoring potential AI deviations, so that all automated decisions are fair, safe, and transparent. You can find more information about our ethics and compliance policies related to AI and AI deviations in our Reporting Channel: https://www.pipefy.com/pt-br/etica-e-compliance/ For any questions or requests, please contact our Help Center: https://help.pipefy.com/

SECURITY METHODOLOGIES

Information Security Management System

EMPHASIS	DETAILS
Goals	The strategic information security objectives (SGSI strategic objectives) are those that Pipefy intends to achieve in accordance with a corporate vision of information security and that are aligned with the objectives mentioned in its Corporate Strategic Plan, among which are: • Promote compliance with laws, rules and regulations relating to the business in its aspects related to Information Security; • Continuously improve the security controls and maturity of the Pipefy Platform to mitigate risks; • Increase knowledge and internal awareness about the need for Information Security for the business.

pipefy Security Overview

Information Security Awareness

METHODOLOGY	DETAILS
Policies	Pipefy has developed a comprehensive set of security policies that cover a variety of topics. These policies are shared and made available to all employees and service providers with access to Pipefy's information assets. Audit Reports are not shared externally, only the results and maturity level of the Pipefy environment.
Training	All new employees attend Security Awareness Training, just as all employees undergo the same training once a year. Furthermore, all employees participate in training on Data Privacy, GDPR and LGPD. All members of the Engineering team also participate once a year (except Security Awareness Training) in a Secure Development Training based on OWASP TOP 10 and SANS 25. Security Awareness is also part of Pipefy's routine, as updates are shared among all teams via email, blog posts, and in presentations during internal events.
Privacy measures	At Pipefy we are aware of your privacy and rights and work to provide you with the best practices and measures to keep your data safe. We comply with the requirements of LGPD and GDPR. And we are working tirelessly, every day, to maintain a high level of maturity in our security measures. You can see more information about Privacy on Pipefy at: • Worldwide Privacy Page: https://www.pipefy.com/privacy-policy/ • Brazilian privacy page: https://www.pipefy.com/pt-br/politica-de-privacidade/ For any questions and requests, please contact us via email: privacidade@pipefy.com. Email from our DPO: dpo@pipefy.com.

Employee Verification

METHODOLOGY	DETAILS
Background scanning	Pipefy conducts background checks on all new employees in accordance with local laws. The background check includes criminal, educational, and employment verification.
Confidentiality Agreements	All new hires are screened during the hiring process and required to sign non-disclosure and confidentiality agreements in accordance with local laws.

ADDITIONAL CERTIFICATIONS AND DOCUMENTATION

CERTIFICATION	DETAILS
ISO 42001	ISO/IEC 42001 standard is the first international standard dedicated to the responsible management of Artificial Intelligence (AI). It establishes a framework of best practices for Artificial Intelligence Management Systems (AIMS), ensuring that organizations adopt technical, ethical, and governance controls to develop, deploy, and operate AI systems in a safe, reliable, and transparent manner.
ISO 27701	ISO 27701 is the international privacy standard that provides a framework for data privacy management. It is a data privacy extension of ISO 27001.

ISO 27018

ISO 27018 is the code of practice for protecting personally identifiable information (PII) in cloud computing services.

SOC 1 and 2 type 2

SOC 1 and 2 are regularly updated reports that focus on controls related to financial controls, security, availability, and confidentiality of a cloud service. Pipefy can share SOC 1 and 2 reports through a signed non-disclosure agreement (NDA).

AWS Qualified Software

Our vendor AWS reviews our infrastructure and application security through Fundamental Technical Review (FTR). This process ensures that our implementation and use of the cloud has been validated by AWS for its technical proficiency and associated customer references.

Consensus Assessments Initiative Questionnaire (CAIQ)

The questionnaire CAIQ provides an industry-accepted way to document what security controls exist on cloud services. This increases security control transparency for current and potential customers, who can then determine whether our services are secure enough for their purposes.

The completed questionnaire can be obtained through a signed non-disclosure agreement (NDA).

REVISION HISTORY

Version	Data	Responsible team	Description
1.0	22/05/2022	PrivSecOps	Document Creation
2.0	20/05/2023	PrivSecOps	Annual review; Addition of scope certifications.
3.0	17/06/2024	PrivSecOps	Annual Review; Template adjustment.
4.0	28/03/2025	PrivSecOps	Annual Review.
5.0	01/09/2025	PrivSecOps	Review with addition of scope certifications.