pipefy

Report

Security Overview

Versão: 1.1 · **Última atualização:** Abril, 2022

Pipefy Data Center & Segurança de Rede

Segurança Física

NOME	DETALHES

Instalações	A infraestrutura física dos provedores de serviços Pipefy é hospedada e gerenciada nos data centers seguros da Amazon e utiliza a tecnologia Amazon Web Service (AWS). A Amazon gerencia continuamente o risco e passa por avaliações recorrentes para garantir a conformidade de acordo com os padrões do setor. As operações do data center da Amazon foram credenciadas sob: ● ISO 27001 ● SOC 1 and SOC 2/SSAE 16/ISAE 3402 (anteriormente SAS 70 Type II) ● PCI Level 1 ● FISMA Moderate ● Sarbanes-Oxley (SOX)
Segurança no Local	Pipefy utiliza data centers com certificação ISO 27001 e FISMA gerenciados pela Amazon. Os data centers da AWS estão alojados em instalações indefinidas e as instalações críticas têm muitas bermas de controle de perímetro de nível militar e retrocessos, bem como outras proteções de limites naturais. O acesso físico é estritamente controlado no perímetro e nos pontos de entrada do prédio por uma equipe 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 funcionários autorizados.
Localização	Os data centers dos provedores de serviços Pipefy estão localizados nos Estados Unidos.

Segurança de rede

NOME	DETALHES
Equipe de Resposta de Segurança	Nossa equipe de resposta de segurança está à disposição para responder a eventos e alertas de segurança e pode ser contatada no e-mail: security@pipefy.com
Proteção	A infraestrutura e o gerenciamento de todos os firewalls são fornecidos por nosso provedor de serviços Amazon AWS. Os firewalls são utilizados para restringir o acesso a sistemas de redes externas e entre sistemas internamente. 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 o risco. Os firewalls baseados em host também oferecem a capacidade de limitar ainda mais as conexões de entrada e saída, conforme necessário.
Verificação de vulnerabilidade	Nossos firewalls gerenciados pelo provedor de serviços evitam spoofing de IP, MAC e ARP na rede e entre hosts virtuais para garantir que o spoofing não seja possível. A detecção de pacotes é evitada pela infraestrutura, incluindo o hipervisor, que não entregará o tráfego a uma interface para a qual não está endereçado. Nosso provedor de serviços utiliza isolamento de aplicativos, restrições de sistema operacional e conexões criptografadas para garantir ainda mais a redução do risco em todos os níveis. A varredura de portas é proibida e cada instância relatada é investigada por nosso provedor de infraestrutura. Quando as varreduras de portas são detectadas, elas são interrompidas e o acesso é bloqueado.

Testes de penetração e avaliações de vulnerabilidade*	Os testes de segurança terceirizados de nosso provedor de serviços são realizados por empresas de consultoria de segurança independentes e de boa reputação. As conclusões de cada avaliação são revisadas com os avaliadores, classificadas em relação ao risco e atribuídas à equipe responsável.
Incidente de Segurança e Resposta	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 apropriada possível. Coletar e analisar informações de log é essencial para solucionar problemas e investigar problemas. Nosso provedor de serviços nos permite analisar três tipos de log principais: logs de sistema, aplicativo e API.
Mitigação de DDoS	A infraestrutura de nosso provedor de serviços fornece técnicas de mitigação de DDoS, incluindo cookies TCP Syn e limitação de taxa de conexão, além de manter várias 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 habilitar controles avançados de mitigação de DDoS quando necessário.
Acesso Lógico	O acesso à Rede de Produção Pipefy é restrito por uma necessidade explícita de conhecimentos. Ele utiliza o mínimo de privilégios, é auditado com frequência e é controlado de perto por nossa equipe de engenharia. Os funcionários que acessam a Rede de Produção Pipefy são obrigados a usar vários fatores de autenticação.

Solicitações de criptografia e autenticação

POLÍTICA	DETALHES
Criptografia em transferência	Toda a comunicação interna e externa é realizada por meio de uma conexão segura com TLS 1.2 ou TLS 1.3.
Criptografia em transferência -- Emails	Todos os emails são enviados pela Sendgrid por meio 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 & Continuidade

POLÍTICA	DETALHES
Tempo de atividade	A disponibilidade do Pipefy foi de 99,92% para o quarto trimestre de 2021 e é monitorada continuamente. Os relatórios de disponibilidade não estão disponíveis em nosso site, mas podem ser fornecidos mediante solicitação.
Redundância	O clustering do provedor de serviços Pipefy e 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 do cliente em caso de interrupção. A plataforma do provedor é projetada para implantar aplicativos dinamicamente em sua nuvem,

	monitorar falhas e recuperar componentes da plataforma com falha, incluindo aplicativos e bancos de dados do cliente.

Segurança do Aplicativo

Desenvolvimento Seguro (SDLC)

POLÍTICA	DETALHES
Controles de Segurança do Framework Ruby on Rails	Utilizamos controles de segurança do framework 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.
QA	Nosso departamento de QA analisa e testa nossa base de código. Engenheiros de aplicativos 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 aplicação

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

Recursos de Segurança do Produto

Desenvolvimento Seguro (SDLC)

RECURSO	DETALHES
Opções de Autenticação	Pipefy oferece suporte a login, SSO e autenticação do Google.
Single sign-on (SSO)	Single sign-on (SSO) permite que você autentique 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 de API & Autenticação	O API do Pipefy é SSL-only 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 de Acesso & Funções	O acesso aos dados em sua conta Pipefy é regido por direitos de acesso e pode ser configurado para definir privilégios de acesso. O Pipefy tem vários níveis de permissão para organização (membro e administrador) e usuários de pipe (startform apenas, membro e administrador).
Segurança de Transmissão	Todas as comunicações com os servidores do provedor de serviços Pipefy são criptografadas usando HTTPS padrão da indústria. Isso garante que todo o tráfego entre você e a Pipefy seja seguro durante o trânsito.

Metodologias adicionais de segurança

Sistema de Gerenciamento de Segurança da Informação

DESTAQUE	DETALHES
Objetivos	Os objetivos estratégicos de segurança da informação (objetivos estratégicos do ISMS) são aqueles que a Pipefy deseja alcançar de acordo com a visão corporativa de segurança, alinhada com os objetivos mencionados no Plano Corporativo Estratégico. Estes objetivos são: • Promote conformidade com leis, regras e regulamentações relacionadas ao negócio e aspectos relacionados com a segurança da informação.

- Melhorar continuamente os controles de segurança e a maturidade da Plataforma Pipefy para mitigar riscos;
- Aumentar o conhecimento e consciência interna sobre a necessidade da segurança da informação para o negócio.

Conscientização de Segurança

METODOLOGIAS	DETALHES
Políticas	Pipefy desenvolveu um conjunto abrangente de políticas de segurança cobrindo uma variedade de tópicos. Essas políticas são compartilhadas e disponibilizadas a todos os funcionários e contratados com acesso aos ativos de informações da 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 funcionários participam de treinamentos de Privacidade de Dados, GDPR e LGPD. Todos os membros da equipe de engenharia também participam uma vez por ano (além do treinamento de conscientização de segurança) em um treinamento de desenvolvimento seguro baseado no OWASP TOP 10 e SANS 25. A conscientização de segurança também faz parte da rotina do Pipefy, pois as atualizações são compartilhadas entre todas as equipes via e-mail, posts em blogs e em apresentações durante eventos internos.
Medidas de Privacidade	Na Pipefy, estamos cientes de sua privacidade e direitos, e trabalhamos para fornecer a você as melhores práticas e medidas para manter seus dados protegidos. Estamos de acordo com os requisitos do LGPD e do 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/

Em caso de dúvidas e solicitações, entre em contato com nosso e-mail: privacy@pipefy.com.

E-mail do nosso DPO: dpo@pipefy.com.

Verificação de Funcionários

METODOLOGIA	DETALHES
Background Checks	Pipefy realiza background checks em todos os novos funcionários de acordo com as leis locais. Os background checks incluem verificação criminal, educacional e de emprego.
Acordos de Confidencialidade	Todos os novos contratados são avaliados durante o processo de contratação e obrigados a assinar acordos de Não Divulgação e confidencialidade (NDA), de acordo com as leis locais.

CERTIFICAÇÕES

CERTIFICAÇÃO	DETALHES
ISO 27001	O padrão ISO 27001 é a estrutura de melhores práticas internacionalmente reconhecida para um Sistema de Gerenciamento de Segurança da Informação (ISMS).
SOC 2	SOC 2 é um relatório atualizado regularmente que se concentra nos controles de relatórios não financeiros relacionados à segurança, disponibilidade e confidencialidade de um serviço em nuvem. A Pipefy pode compartilhar o relatório SOC 2, por meio de um acordo de confidencialidade (NDA) devidamente assinado.