RELATÓRIO TÉCNICO

Segurança e privacidade da Asana

Como a Asana protege os seus dados

Índice

Última atualização: outubro de 2022[1]

[1] Este relatório técnico descreve o estado atual da segurança da Asana, que está sujeito a alterações com lançamentos futuros de recursos e produtos.

Introdução

Os clientes confiam os seus dados à Asana para poderem se dedicar ao trabalho mais importante para os seus negócios. É por esse motivo que o nosso foco não é apenas criar uma solução de gestão colaborativa do trabalho que seja fácil de usar, preocupamo-nos também com a segurança dos dados dos nossos clientes.

Neste relatório técnico, você verá como a Asana prioriza a segurança, a disponibilidade e a confidencialidade por meio de:

- Infraestrutura
- Produto
- Ambiente físico e operacional
- Privacidade, certificações e conformidade.

Embora a maior parte deste relatório técnico seja aplicável a qualquer tipo de plano da Asana, ele foi elaborado levando em consideração os planos Asana pagos: Premium, Business e Enterprise.[2] Serão assinalados os recursos que não estiverem disponíveis em todos os planos.

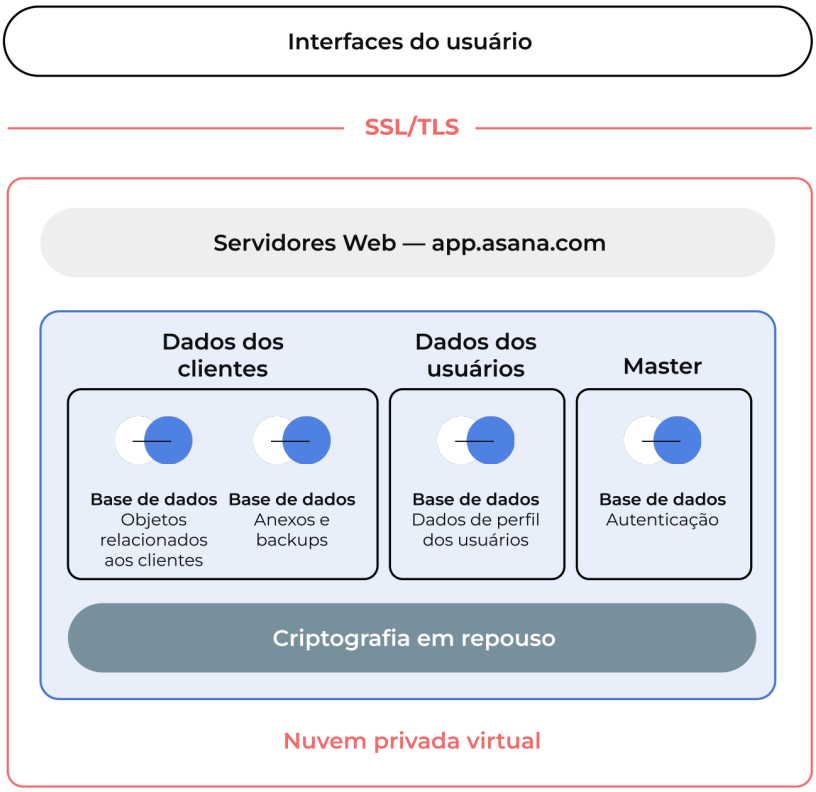
[2] Para obter mais informações sobre os planos Asana, acesse https://asana.com/pt/pricing.

Infraestrutura

A Asana utiliza serviços de computação em nuvem, principalmente da Amazon Web Services (AWS), como componentes essenciais da plataforma Asana.

A AWS faz a gestão da segurança e da conformidade da infraestrutura de computação em nuvem, e a Asana faz a gestão da segurança e da conformidade do software e dos dados armazenados na infraestrutura de computação em nuvem. Consulte o Modelo de responsabilidade compartilhada da AWS.[3]

A Asana usa o Virtual Private Cloud da Amazon, e a sua arquitetura de rede foi projetada para ser segura, escalável e facilmente administrável mediante o uso dos serviços de rede e dos componentes essenciais fornecidos pela AWS. O serviço *Elastic Compute Cloud* (EC2) da Amazon opera a maior parte da plataforma Asana e oferece uma maneira confiável, escalável e segura de processar os dados dos clientes. Veja a seguir um diagrama simplificado da infraestrutura da Asana.



[3] https://aws.amazon.com/pt/compliance/shared-responsibility-model/

A nossa infraestrutura de produção é protegida, de modo que apenas os nossos computadores de balanceamento de carga tenham permissão para receber o tráfego externo da Web. Cada *host* recebe uma função, e são usados grupos de segurança para determinar o tráfego esperado entre essas funções.

Servidores Web

A capacidade segura, confiável e baseada em nuvem da Amazon EC2 constitui a maior parte do nosso cenário de servidores Web. Estes processam os dados dos clientes e entregam a funcionalidade do aplicativo aos usuários, ao mesmo tempo que interagem com outras partes da nossa infraestrutura.

Bancos de dados

Os bancos de dados consistem no Relational Database Service (RDS) da Amazon e executam um banco de dados MySQL gerido.

Master

Armazena dados, como senhas criptografadas (bcrypt com hashes e salts) e informações de autenticação dos diversos usuários. Também armazena outros metadados que permitem o roteamento de tráfego.

Dados dos clientes

Armazenam todas as informações inseridas ou enviadas pelos clientes para a Asana, incluindo projetos e tarefas.

Dados dos usuários

Armazenam as informações relacionadas a perfis de usuários, como nome e endereço de e-mail.

Armazenamento de arquivos

Os servidores de armazenamento operam no Simple Storage Server (S3) da Amazon. Eles armazenam anexos e backups de bancos de dados. Anexos são quaisquer arquivos enviados a tarefas na Asana a partir de um computador. Os anexos provenientes das plataformas de colaboração de conteúdo hospedadas na nuvem são criados como links que levam a essas plataformas, mas não são mantidos nos servidores de armazenamento da Asana.

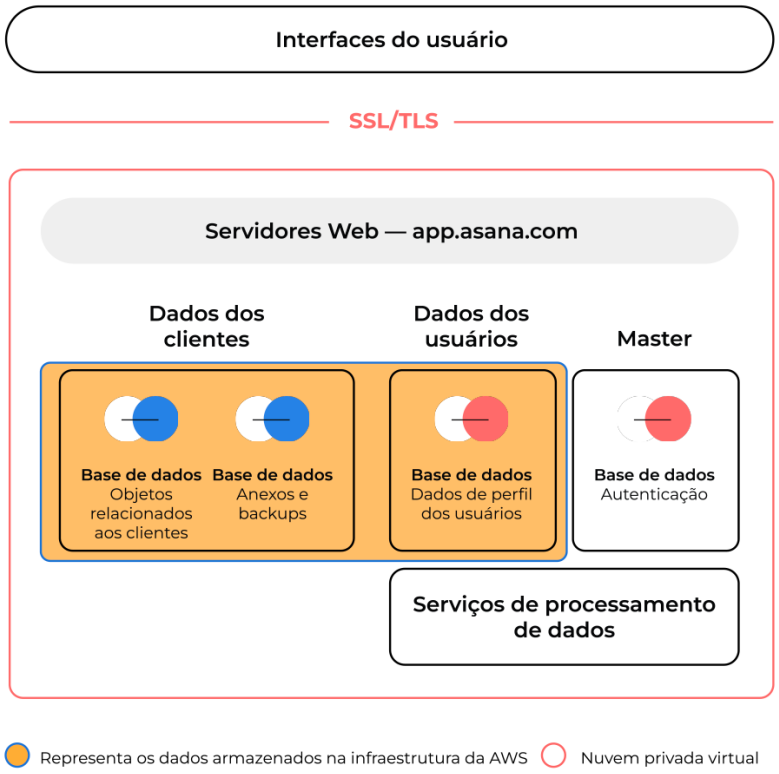
Locais dos centros de dados

A Asana oferece centros de dados da AWS em vários locais para os clientes do plano Asana Enterprise que precisam ter os seus dados armazenados em um local específico:

- Infraestrutura europeia: os dados dos clientes e a maioria dos dados dos usuários serão armazenados na região da AWS em Frankfurt (Alemanha), com backups armazenados na região da AWS em Dublin (Irlanda).
- Infraestrutura australiana: os dados dos clientes e a maioria dos dados dos usuários serão armazenados na região da AWS em Sydney (Austrália), com backups armazenados na região da AWS em Dublin (Irlanda).
- Infraestrutura no Japão: os dados dos clientes e a maioria dos dados dos usuários serão armazenados na região da AWS em Tóquio (Japão), com backups armazenados na região da

AWS em Osaka (Japão).

Veja a seguir um diagrama simplificado da infraestrutura da Asana para os clientes que solicitarem residência dos dados.



Segurança de dados

Criptografia

As conexões com o app.asana.com são codificadas com criptografia de 128-bit e oferecem suporte ao protocolo TLS 1.2 e versões superiores. As conexões são codificadas e autenticadas com AES_128_GCM e usam ECDHE_RSA como o mecanismo de troca de chaves. A Asana oferece suporte a *forward secrecy* e AES-GCM e proíbe conexões inseguras que usem os protocolos RC4 ou TLS 1.1 e versões anteriores a estas. Logins e transferências de dados confidenciais são realizados apenas sob o protocolo TLS. A Asana garante a criptografia em repouso com chaves secretas AES de 256-bit.[4]

Gestão de chave empresarial

A Asana oferece a determinados clientes Enterprise a opção de usar a sua própria chave de criptografia para criptografar os dados na Asana. Os clientes podem usar o Key Management Service (KMS) da Amazon Web Services (AWS) para as suas chaves de criptografia. Clientes que usam a gestão de chave empresarial (EKM) na Asana controlam as chaves de criptografia dos seus bancos de dados do domínio, anexos, buscas e a maioria dos dados de usuários da sua organização. Para saber mais e configurar a

[4]Para mais informações sobre quais dados na Asana são criptografados, consulte o Diagrama na página 6.

gestão de chave empresarial na Asana, entre em contato com a nossa equipe de vendas pelo e-mail sales@asana.com.

Multilocação

A Asana é um aplicativo Web multilocatário, o que significa que a infraestrutura é compartilhada entre as instâncias do cliente. A autenticação de contas, a separação lógica de campos do banco de dados e os controles de gestão de sessões são implementados de maneira a limitar o acesso dos clientes somente aos dados relacionados com a organização correspondente.

Escalabilidade e confiabilidade

A Asana usa a Amazon Web Services, que proporciona a escalabilidade do serviço. Os bancos de dados são replicados de maneira sincronizada, o que permite a recuperação rápida de falhas no banco de dados. Como precaução adicional, são capturados instantâneos regulares do banco de dados que são transferidos com segurança para um centro de dados que atua como cópia de segurança. Com isso, podemos restaurar o acesso do cliente, mesmo se ocorrer uma falha na região primária da AWS.

Grau de disponibilidade do sistema

A Asana se compromete a uma disponibilidade de serviço de 99,9% para os clientes Enterprise. Os clientes podem visualizar e inscrever-se para receber atualizações de status do sistema em status.asana.com, que mostra a disponibilidade dos nossos aplicativos móveis, aplicativo Web e API das últimas 12 horas, 7 dias, 30 dias e 365 dias.

Backups

São capturados instantâneos do banco de dados diariamente. Os backups contam com a mesma proteção dos bancos de dados de produção. Garantimos o armazenamento inter-regional de backups.

Recursos de segurança do produto

A Asana fornece aos usuários e administradores os recursos necessários para proteger os seus dados. Esses recursos proporcionam controle administrativo abrangente e visibilidade quanto aos dados dos clientes. A disponibilidade dos recursos a seguir varia conforme o plano Asana. Veja os planos em asana.com/pt/pricing.

Administradores

Os administradores podem gerir as equipes para adicionar e remover membros e convidados à medida que ingressam e deixam a empresa ou o fluxo de trabalho. Eles também podem usar a nossa API de administrador para gerir exportações de domínios, configurações, permissões, aplicativos de terceiros e configurações de equipes e usuários.

Provisionamento e desprovisionamento de usuários

A Asana permite que os usuários e administradores controlem quem tem acesso aos seus dados.

- Os usuários e administradores podem convidar membros e adicionar convidados (membros externos) às suas organizações e equipes.
- Os administradores podem remover qualquer membro ou convidado no Painel do administrador.

Além disso, os clientes do plano Enterprise podem integrar a Asana ao seu provedor de identidade na nuvem por meio do padrão do sistema para gestão de identidade entre domínios (SCIM, System for Cross-domain Identity Management), para adicionar e remover usuários conjuntamente com o restante das suas soluções de SaaS.[5]

Segurança do login

Os administradores da Asana podem determinar o mecanismo usado pelos usuários para fazer login nas suas contas Asana. Há três opções diferentes: credenciais da Asana, SSO (Logon único) do Google ou o SSO via SAML 2.0.

Proteções de senhas

Quando os usuários têm permissão para fazer login nas suas contas usando as credenciais da Asana, os administradores podem especificar a força necessária para as senhas. Exigir senhas "fortes" obrigará os usuários a utilizar, no mínimo, 8 caracteres que contenham três dos seguintes elementos: letra minúscula, letra maiúscula, números e caracteres especiais. A personalização de senhas permite que os administradores modifiquem a complexidade dos requisitos de senhas no seu domínio.[6] Os administradores também podem impor uma redefinição de senha para todos os usuários da organização.

[5] https://asana.com/pt/guide/help/premium/scim
[6] https://asana.com/pt/guide/help/premium/authentication#gl-force

Autenticação de dois fatores (2FA)

Os administradores de planos Enterprise podem solicitar a autenticação de dois fatores para os logins na Asana.[7]

SSO do Google

Os administradores podem exigir que os usuários da organização façam login na Asana usando a sua conta do Google Workspace.

Logon único (SSO) via SAML

Os administradores de um plano Enterprise podem configurar um provedor de identidade (IdP) próprio e solicitar que os usuários façam login na Asana com as credenciais da conta do idP na nuvem. Isso é configurado por meio do padrão de autenticação SAML. Os administradores Enterprise podem definir a duração do tempo limite do SAML no painel do administrador na Asana.

API de registro de auditorias

A API de registro de auditorias da Asana permite que os administradores de planos Enterprise detectem ameaças de segurança na Asana por meio do Splunk, Panther ou de qualquer provedor de gestão de eventos e informações de segurança (SIEM) da sua preferência com alguns ajustes. Com a nossa integração pronta para uso com o Splunk e o Panther, as equipes de TI podem visualizar e monitorar as principais atividades relacionadas à conformidade na Asana diretamente do painel do Splunk. Além disso, os administradores podem proteger de maneira proativa os dados da organização e atuar ao serem identificadas atividades suspeitas com o uso de alertas oportunos e personalizáveis.[8]

Gestão de espaços de trabalho aprovados

A funcionalidade da Asana para Gestão de espaços de trabalho aprovados permite que os administradores Enterprise limitem o uso da Asana a um conjunto de espaços de trabalho aprovados em uma rede ou dispositivo controlado. Isto também está disponível por meio de uma parceria com a Netskope.

Permissões de acesso

Os administradores e usuários podem convidar outras pessoas a aceder aos seus dados. Os usuários podem ser convidados a participar de uma organização com privilégios distintos. Os convites feitos limitam-se ao elemento específico (tarefa, projeto, equipe ou organização), com diferentes tipos de acesso. As permissões para os usuários são definidas no âmbito do elemento e não do usuário, ou seja: um usuário pode ter acesso somente para comentar em alguns conteúdos, outros podem estar completamente ocultos a ele ou “disponíveis mediante solicitação” e, em determinados elementos, o usuário pode ter acesso pleno para visualizar e modificar o seu conteúdo. É possível compreender a fundo os detalhes de cada elemento e tipo de permissão no nosso Guia Asana: asana.com/pt/guide.

Elementos da Asana

[7] https://asana.com/pt/guide/help/premium/admin-console-mandatory-2fa
[8] https://asana.com/pt/guide/help/api/audit-log-api

Tarefas

As tarefas na Asana podem ser privadas, públicas, estar contidas em um projeto privado ou em um projeto público.

Tarefa:	Acessibilidade:
Tarefa privada	Somente aos colaboradores da tarefa
Tarefa pública	Todos os membros da organização
Tarefa em um projeto privado	Colaboradores da tarefa e membros do projeto
Tarefa em um projeto público	Colaboradores da tarefa, membros do projeto e membros da equipe
Subtarefa	Colaboradores da tarefa e pessoas com acesso à tarefa principal

Projetos

Os projetos na Asana podem ser privados ou públicos. Se um usuário tem acesso a um projeto, significa que ele pode acessar todas as tarefas e conversas contidas nesse projeto. Os usuários podem ser adicionados a um projeto com acesso para editar ou somente para comentar. Os administradores de planos Enterprise podem definir um nível de privacidade padrão para as equipes da sua organização.

Projeto:	Acessibilidade:
Projeto privado	Membros do projeto
Projeto público	Membros da equipe e do projeto
Projeto público em uma equipe pública	Membros da organização, da equipe e do projeto

Equipes

As equipes na Asana podem ser ocultas, públicas ou de participação por solicitação. Se um usuário pertence a uma equipe, significa que ele pode acessar todas as conversas e projetos públicos contidos nessa equipe.

Equipe:	Acessibilidade:	Podem participar:
Oculta	Membros da equipe	Não
Pública para a organização	Membros da equipe e da organização	Sim
Participação por solicitação	Membros da equipe	Sujeito a aprovação

Organizações

As organizações na Asana são os elementos de nível mais elevado, contendo nelas todas as equipes, projetos e tarefas.

Usuários

Os usuários da Asana recebem contas individuais que são vinculadas ao seu endereço de e-mail e cujo acesso aos diferentes elementos de dados é determinado conforme mencionado anteriormente. Por padrão, as contas dos usuários têm acesso a uma organização de acordo com o seu domínio de e-mail.

Membros com acesso completo

A associação à organização é feita com base no domínio do endereço de e-mail. Para se tornar membro de uma organização, é necessário ter um endereço de e-mail com um domínio aprovado pela respectiva organização.

Um membro de uma organização pode:

- Criar novas equipes.
- Ver a lista completa das equipes às quais pode pedir para participar dentro da organização.
- Ver nomes e endereços de e-mail de outros membros e convidados da organização.
- Acessar projetos e tarefas que foram definidos como públicos para a organização.

Convidados

É possível colaborar com clientes, terceirizados ou qualquer outra pessoa que não tenha um endereço de e-mail com um domínio aprovado pela organização. Esses usuários passam a ser convidados da organização. Os convidados têm acesso limitado à organização e podem ver apenas o que for explicitamente compartilhado com eles.

Um convidado da organização só pode participar de equipes se receber convites específicos a cada uma delas. Os convidados não podem criar novas equipes ou ver e pedir para participar de qualquer outra equipe.

Membros com acesso limitado

Cada equipe tem os seus próprios membros e projetos. Os membros que não têm acesso a todos os projetos da equipe aparecem como *Membros com acesso a projetos específicos* na guia Membros das configurações da equipe.

Membros com acesso a projetos específicos podem ver os projetos e tarefas a que foram adicionados, mas não têm acesso às mensagens ou a outros projetos da equipe.

Gestão de convidados

Os administradores do plano Enterprise podem determinar quem tem permissão para convidar membros externos (convidados). Os administradores têm as três opções abaixo ao decidir quem pode adicionar convidados à organização:

- Somente administradores
- Administradores e membros da organização
- Todos (inclui membros e convidados da organização).

Gestão de administradores de aplicativos

Os administradores do plano Enterprise podem determinar que integrações de terceiros podem ser utilizadas pelos usuários com suas contas Asana, bem como bloquear as integrações indesejadas. Acesse asana.com/pt/apps para saber quais são os aplicativos de terceiros disponíveis.[9]

Controle de dados

Os clientes podem exportar ou excluir dados da Asana e automatizar exportações de domínios completos usando a nossa API.

[9] https://asana.com/pt/guide/help/premium/app-management

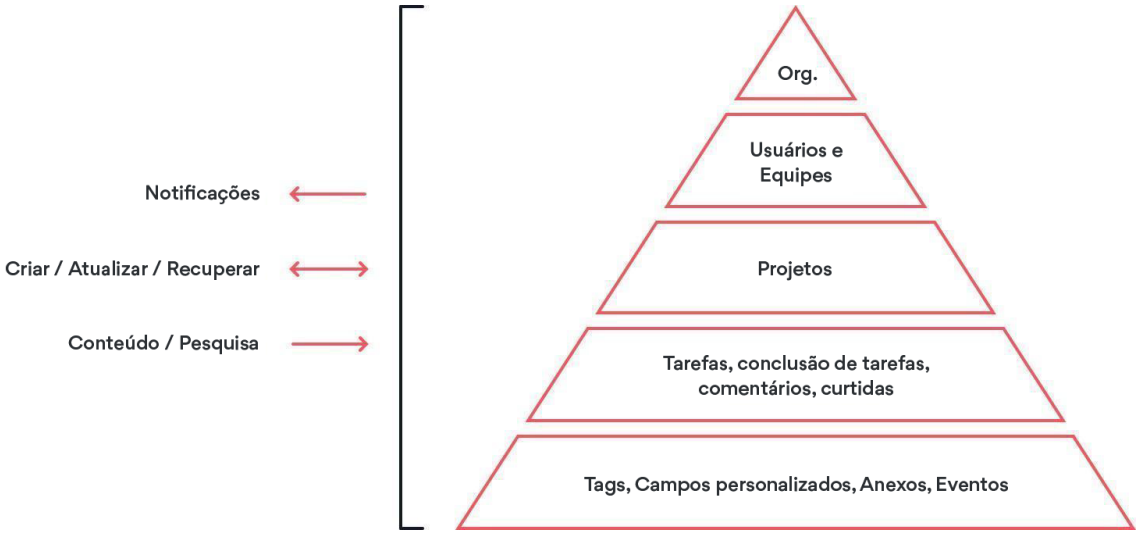
Plataforma Asana

Integrações

A Asana permite que os usuários acessem as suas contas por meio de uma API (Interface de Programação de Aplicativos, na sigla inglesa)[10]. A API da Asana consiste em uma interface RESTful, que permite atualizar e acessar de forma programática muitos dos seus dados na plataforma, bem como reagir automaticamente quando ocorrem alterações. Fornece URLs previsíveis para acessar os recursos e usa as funcionalidades HTTP incorporadas para receber comandos e retornar respostas. Isso facilita a comunicação com a Asana a partir de uma ampla variedade de ambientes, que abrangem desde utilitários da linha de comando a plugins de navegadores e aplicações nativas. Os clientes podem usar essas APIs para criar soluções personalizadas ou para fazer a integração com outros softwares. A Asana oferece suporte a OAuth 2.0 ou a Token de acesso pessoal como métodos de autenticação com a API.

Para saber mais sobre a API da Asana, acesse asana.com/pt/developers.

A ilustração a seguir apresenta um resumo das ações que podem ser executadas e dos elementos com os quais é possível trabalhar.



Por padrão, qualquer software ou script terá as mesmas permissões que o usuário que o está executando. Os dados disponíveis limitam-se àqueles a que o usuário tem acesso. Se for necessário conceder acesso adicional, clientes do plano Enterprise podem usar as contas de serviço.

[10] https://asana.com/pt/guide/help/api/api

Contas de serviço

Os clientes do plano Asana Enterprise podem usar contas de serviço para acessar todos os seus conteúdos. Por exemplo, as contas de serviço podem ser usadas para realizar uma exportação completa dos dados da organização ou para monitorar as atividades das equipes. Mais informações podem ser obtidas no Guia[11].

Aplicativos de terceiros

A API da Asana viabiliza o uso com centenas de integrações prontas, que os clientes podem usar para aprimorar ou complementar a sua experiência na Asana. A Asana integra-se a diversas ferramentas para agilizar os fluxos de trabalho dos clientes e aumentar a produtividade. É possível também integrar ferramentas externas de outros fornecedores para:

- Sincronização de mensagens entre os aplicativos
- Automatização do fluxo de trabalho
- Extensões da plataforma
- Desenvolvimento de software
- Importações de dados
- Compartilhamento de arquivos
- Geração de relatórios
- Monitoramento de tempo
- Recebimento de dados

Um diretório contendo os aplicativos de terceiros pode ser visto em asana.com/pt/apps.

[11] https://asana.com/pt/guide/help/premium/service-accounts

Segurança do aplicativo

Proteção do código que desenvolvemos

A equipe de segurança dos aplicativos criados pela Asana trabalha continuamente para aprimorar os métodos de identificação de falhas de segurança nos nossos aplicativos, com a ajuda de pesquisadores internos e externos de segurança, ferramentas de última geração, modelagem de ameaças e testes de segurança. Assim que uma falha de segurança é identificada e confirmada, os responsáveis pela gestão de vulnerabilidades são informados para a solucionarem em tempo hábil.

O serviço da Asana consiste em um software como serviço on-line. Os usuários podem acessar os seus dados por meio de um navegador da Internet, aplicativo para dispositivos móveis (Android e iOS) ou API (Interface de Programação de Aplicativos, na sigla em inglês).

Os serviços e elementos que compõem a Asana são escritos principalmente em JavaScript, TypeScript, Python e Scala, com base na estrutura de aplicação React. A Asana foi desenvolvida de acordo com as boas práticas de segurança definidas pela Fundação OWASP e com uma abordagem de "segurança desde a concepção" em todos os momentos. Portanto, foram implementados mecanismos abrangentes para evitar riscos à segurança, incluindo, entre outros, os tópicos a seguir:

- Injeção
- Quebra de autenticação
- Exposição de dados confidenciais
- Entidades externas XML (XXE)
- Quebra de controle de acesso
- Configuração incorreta de segurança
- Cross-Site Scripting (XSS)
- Desserialização insegura
- Uso de componentes com vulnerabilidades conhecidas
- Registro e monitoramento insuficientes
- Cross-Site Request Forgery (CSRF)
- Redirecionamentos e encaminhamentos não validados

Anualmente, entidades externas independentes realizam auditorias na Asana quanto aos dez principais riscos de segurança em aplicativos Web identificados pela OWASP. Também executamos testes de segurança internamente em áreas que requerem uma análise mais profunda quanto à eficácia dos nossos controles de segurança.

Proteção do código de terceiros

Para garantir o uso das versões mais seguras das bibliotecas e componentes de terceiros para compor a nossa experiência do produto, a equipe de segurança de aplicativos realiza um programa que atribui a responsabilidade às nossas equipes de engenharia para instalar atualizações às bibliotecas e componentes de terceiros em tempo hábil quando houver o risco de afetar a postura de segurança do nosso produto.

Segurança operacional

Segurança das informações da Asana

A Asana mantém um programa formal de gestão da segurança da informação com uma equipe de segurança dedicada que presta contas ao diretor de segurança da Asana. Esta organização é responsável por implementar controles de segurança e monitorar a Asana quanto a atividades suspeitas.

Informações confidenciais

A Asana trata todos os dados dos clientes como confidenciais. As nossas políticas e procedimentos restringem o acesso a informações confidenciais aos funcionários que devem ter acesso a esse tipo de informação para realizar o seu trabalho, e apenas nos casos em que o acesso a tais informações se fizer necessário para prestar um serviço específico aos clientes. Nessas condições, os funcionários são orientados a acessar somente o mínimo de informações necessárias ao desempenho da tarefa em questão.

Recursos humanos

Todos os funcionários e terceirizados da Asana devem assinar um contrato de confidencialidade e de direitos autorais sobre invenções. Além disso, os funcionários são submetidos a um treinamento formal de conscientização sobre segurança no ato da contratação e anualmente nos anos subsequentes.

Todos os engenheiros da Asana assinam um contrato de política de acesso a dados que define o acesso e uso apropriados dos dados. Além disso, dispomos de gateways para os pontos de entrada aos dados dos clientes: todos os acessos a dados são registrados e armazenados indefinidamente.

A Asana possui uma política disciplinar e de sanções por violações à política.

Revisões e política de acesso dos usuários

Trimestralmente, a direção revisa o acesso dos usuários aos sistemas com abrangência relevante para assegurar uma adequação constante e revogar os acessos que já não forem necessários. Após o desligamento de funcionários, o seu acesso também é removido.

Segurança física

Escritórios da Asana

Os nossos escritórios são protegidos por cartões de controle de acesso, os acessos são registrados, e todos os escritórios dispõem de sistemas de alarme contra invasão. Os visitantes devem registrar-se na recepção. Todos os funcionários são orientados a informar quaisquer atividades suspeitas, acessos não autorizados às instalações ou incidentes de roubo/perda de objetos.

Segurança dos centros de dados

A Asana conta com os controles físicos e ambientais da AWS.[12]

[12] https://aws.amazon.com/pt/compliance/data-center/controls/

Segurança da rede

Monitoramos a disponibilidade da nossa rede de escritórios e os dispositivos contidos nela. Coletamos num local central os registros produzidos por dispositivos de rede, como firewalls, servidores DNS, servidores DHCP e roteadores. Os registros de rede são armazenados para o dispositivo de segurança (firewall), os pontos de acesso sem fio e os comutadores (switches).

Segurança de TI

Todos os computadores portáteis e estações de trabalho são protegidos com criptografia de disco completo e são provisionados a partir de uma imagem administrada de forma centralizada. Aplicamos atualizações periódicas aos dispositivos dos funcionários e monitoramos malwares nas estações de trabalho. Também podemos aplicar patches críticos de segurança e apagar qualquer máquina remotamente por meio de um gestor de dispositivos. Sempre que possível, utilizamos a autenticação de dois fatores para proteger ainda mais o acesso à nossa infraestrutura corporativa. A Asana realiza verificações de segurança periodicamente.

Gestão de riscos e vulnerabilidades

A Asana mantém um processo contínuo de gestão de riscos que visa identificar as vulnerabilidades nos sistemas da Asana e avaliar, de forma proativa, ameaças novas e emergentes às operações da empresa.

Há também um processo de verificação de vulnerabilidades para sistemas externos e internos no ambiente de produção. A equipe de segurança da Asana realiza verificações de vulnerabilidade com periodicidade mínima trimestral e corrige as vulnerabilidades em função do risco apresentado. As verificações de vulnerabilidade também são realizadas após qualquer alteração significativa no ambiente de produção, conforme determinado pelo diretor de segurança.

Testes de penetração

A Asana contrata anualmente uma empresa profissional de avaliação de segurança (testadores de penetração) para identificar qualquer vulnerabilidade que possa afetar o nosso produto, dados e sistemas. Esses testes abrangem a nossa infraestrutura, aplicativos (Web e móveis) e rede interna. Corrigimos os problemas encontrados e disponibilizamos um relatório dos resultados para análise pelos clientes.

Recompensas por bugs

Mantemos um programa externo de recompensas por bugs[13] no qual concordamos em remunerar os pesquisadores de segurança que descobrirem vulnerabilidades. A nossa equipe de segurança faz regularmente a triagem dos envios e paga o dobro do valor pela mesma gravidade de descoberta em comparação com os nossos concorrentes. Com isso, conseguimos dez vezes mais engajamento do que os concorrentes, o que acaba resultando em um produto mais seguro.

[13] http://asana.com/bounty

Ciclo de desenvolvimento do software

A Asana dispõe de vários programas de segurança ligados a diferentes estágios do ciclo de desenvolvimento do software, para que os nossos engenheiros contem com o melhor controle de segurança do setor para desenvolver um produto que proteja eficazmente os nossos clientes.

O controle ao nível da ideação e criação serve para identificar mudanças planejadas que possam afetar a nossa postura de segurança. Todos os esforços relacionados ao desenvolvimento de novos softwares passam por um processo padronizado, e as mudanças identificadas como de risco médio a alto são analisadas e debatidas com a equipe de segurança do produto antes de se passar à etapa de implementação. Isto ajuda a identificar possíveis problemas de projeto com antecedência e evitar que os clientes venham a ser afetados.

O controle ao nível da implementação e lançamento assegura que os desenvolvedores da Asana disponham de métodos e ferramentas que ajudem a identificar e evitar falhas de segurança nos seus códigos. A Asana usa o sistema de controle de revisões Git. Modificações feitas à base de códigos da Asana são submetidas a um conjunto de testes automatizados. Além disso, alterações identificadas como de alto risco passam por uma etapa de análise e verificação manual realizada pela equipe de segurança do aplicativo. Ao serem aprovadas pelo sistema automatizado de teste, as alterações de código são inicialmente aplicadas a um servidor de teste, no qual os colaboradores da Asana podem testar as mudanças antes de eventualmente implementá-las nos servidores de produção e na nossa base de clientes. É realizada também uma verificação de segurança específica para modificações e recursos particularmente sensíveis. Os engenheiros da Asana podem ainda eleger atualizações críticas a serem implementadas imediatamente nos servidores de produção.

Além de haver uma lista onde são publicadas todas as modificações feitas aos controles de acesso, temos um conjunto de testes automatizados para verificar se as regras de controles de acesso estão escritas corretamente e se são aplicadas conforme esperado.

Resposta a incidentes

A Asana mantém um Plano de resposta a incidentes elaborado para estabelecer uma resposta sensata e consistente a incidentes de segurança e a episódios suspeitos de segurança que envolvam a destruição acidental ou ilegal, perda, roubo, alteração, divulgação não autorizada ou acesso a dados proprietários ou pessoais transmitidos, armazenados ou processados pela Asana. Tais procedimentos de resposta a incidentes especificam como a Segurança da Asana deve fazer as triagens, investigar, corrigir e gerar relatórios sobre os incidentes de segurança. A Asana tem contrato firmado com empresas terceirizadas de análises forenses digitais e resposta a incidentes em caso de violação dos dados.

Recuperação de desastres e continuidade dos negócios

A Asana preparou um plano de continuidade do negócio para interrupções prolongadas no serviço causadas por desastres imprevisíveis ou inevitáveis, com o objetivo de restaurar os serviços tanto quanto possível e dentro de um prazo razoável. A Asana documentou um conjunto de políticas e procedimentos de recuperação de desastres para possibilitar a recuperação ou continuidade da infraestrutura e dos sistemas de tecnologia vitais após um desastre. A Asana realiza testes anuais do plano de recuperação de desastres e publica os resultados para os seus clientes.

Os principais centros de dados da Asana estão hospedados na AWS localizada na Virgínia, nos Estados Unidos. Clientes elegíveis (planos Enterprise) podem solicitar que os seus dados sejam armazenados

em Frankfurt (Alemanha), Sydney (Austrália) ou Tóquio (Japão). Caso ocorra a perda de um único centro de dados da AWS, os procedimentos de recuperação empregam os nós disponíveis em outro centro de dados. Como plano de contingência no evento de grandes catástrofes, há um local de recuperação de desastres localizado em um centro de dados da AWS em Ohio (para os dados que se encontram nos EUA), em Dublin, na Irlanda (para os dados na UE e na Austrália) e em Osaka (para os dados no Japão).

Retenção e remoção de dados

A Asana retém as informações dos clientes pelo tempo necessário para cumprir as finalidades descritas na nossa Política de privacidade. Mediante solicitação do representante autorizado de um cliente, a que se seguirá uma verificação, é possível fazer a exportação ou exclusão de domínio dos seus dados. Além disso, a Asana pode concordar em preservar a confidencialidade de quaisquer dados armazenados, e somente processará ativamente tais dados de clientes após a data da solicitação em cumprimento às leis a que está sujeita.

Monitoramento

A Asana usa o CloudWatch e o CloudTrail da Amazon em conjunto com scripts personalizados que extraem dados importantes dos registros e os enviam para os seus serviços de monitoramento. A Asana monitora a capacidade de utilização da infraestrutura física e computacional tanto internamente quanto para os clientes, de modo a assegurar que a entrega dos serviços corresponda aos acordos de nível de serviço. Dispomos de verificações de segurança automatizadas na nossa rede e aplicativos, além de monitoramento a nível do kernel e alertas sobre os servidores. É também executado semanalmente um script de monitoramento para confirmar que as alterações de código foram revisadas corretamente.

Determinados registros de aplicativos e máquinas são retidos indeterminadamente e mantidos no armazenamento de longo prazo do S3, em circunstâncias normais. Os registros de máquina mais detalhados são armazenados somente na máquina que os gerou e costumam ser mantidos por duas semanas.

Gestão de fornecedores e subprocessadores

A Asana toma medidas razoáveis para selecionar e manter somente fornecedores de serviços terceirizados que respeitarão e implementarão as medidas de segurança conforme determinadas nas nossas políticas. Antes de implementar um software ou poder usar um fornecedor de softwares na Asana, as equipes de segurança, privacidade e TI da Asana revisam cuidadosamente os protocolos de segurança, as políticas de retenção de dados, as políticas de privacidade e o histórico de segurança dos fornecedores. Qualquer fornecedor que não demonstre ter a capacidade de proteger adequadamente os dados e usuários finais da Asana poderá ser rejeitado. São realizadas anualmente reavaliações dos fornecedores críticos.

Como condição para permitir que um subprocessador processe dados de clientes, a Asana (e suas afiliadas, se for o caso) firmará um contrato por escrito com cada subprocessador, estabelecendo obrigações de proteção de dados que tenham, pelo menos, o mesmo nível de proteção que as medidas técnicas e organizacionais que a Asana tem em vigor para proteger os dados pessoais dos clientes contra destruição, perda, alteração, acesso ou divulgação acidentais ou ilícitas.

Os clientes podem se inscrever para receber notificações sobre as mudanças nos nossos subprocessadores e ver os nossos subprocessadores atuais na página que mantemos sobre o assunto.[14]

[14] https://asana.com/pt/terms#subprocessors

Privacidade, certificações e conformidade

Declaração de privacidade

A Declaração de privacidade da Asana comunica as nossas práticas atuais de processamento de dados e é atualizada regularmente. A Declaração de privacidade descreve os dados que coletamos e processamos e fornece informações sobre como os indivíduos podem exercer os seus direitos de privacidade nos termos das leis aplicáveis.[15]

Transferências internacionais de dados

A legislação de proteção de dados da União Europeia exige que as organizações utilizem procedimentos legalmente reconhecidos para transferir dados da União Europeia para países que não possuam uma estrutura equiparável de proteção de dados, o que inclui os Estados Unidos.

Embora a transferência de dados pessoais da União Europeia e da Suíça para os Estados Unidos, nos termos dos enquadramentos do Escudo de Privacidade estabelecido entre a União Europeia e os Estados Unidos, e entre a Suíça e os Estados Unidos, não esteja mais em vigor, o Adendo de Processamento de Dados da Asana inclui as cláusulas contratuais-tipo, que continuam a vigorar como um mecanismo jurídico que rege a transferência de dados pessoais para fora do espaço econômico europeu. Além disso, a Asana também emprega as cláusulas contratuais-tipo com todos os seus subprocessadores.

A Asana adotou diversas medidas complementares para proteger dados pessoais transferidos do espaço econômico europeu, como os relacionados neste documento. Seguimos as melhores práticas do setor, por exemplo, a transferência criptografada de dados da UE para os EUA feita pela Asana através da plataforma da Asana.

Embora a Asana já não possa fazer transferências de dados do espaço econômico europeu e da Suíça ao abrigo do Escudo de Privacidade, optou-se por manter a sua certificação quanto ao Escudo de Privacidade para que se continue a proteger os dados já transferidos nos termos desse enquadramento e, também, para reafirmar o nosso compromisso com suas medidas de segurança para proteção dos dados.

As diretrizes regulamentares do espaço econômico europeu continuam a se desenvolver, e temos acompanhado atentamente as novas orientações das autoridades de proteção de dados. A Asana permanece comprometida com a privacidade dos seus clientes e continuará a assegurar a sua conformidade com as leis de proteção de dados.

RGPD

O Regulamento Geral de Proteção dos Dados (RGPD) é uma lei europeia que estabelece proteções aos dados pessoais dos residentes da UE, em vigor desde 25 de maio de 2018. De acordo com o RGPD, as organizações que coletam, mantêm, utilizam ou processam os dados pessoais dos residentes da UE (independentemente da localização da organização) devem implementar determinadas garantias de privacidade e segurança para esses dados. A Asana definiu um programa abrangente de conformidade com o RGPD e está comprometida a estabelecer parcerias com os seus clientes e fornecedores para reforçar a conformidade com o RGPD. Algumas das medidas significativas adotadas pela Asana para alinhar as suas práticas ao RGPD incluem:

[15] https://asana.com/pt/terms#privacy-policy

- Revisões das nossas políticas e contratos com parceiros, fornecedores e usuários.
- Aprimoramento dos nossos procedimentos e práticas de segurança.
- Profunda análise e mapeamento dos dados que coletamos, usamos e compartilhamos.
- Criação de uma documentação interna mais robusta sobre privacidade e segurança.
- Treinamento dos funcionários sobre os requisitos do RGPD e boas práticas gerais de privacidade e segurança.
- Avaliação e elaboração minuciosas de um processo de resposta e de uma política dos direitos dos titulares dos dados. Fornecemos a seguir outras informações sobre os aspectos centrais do programa de conformidade com o RGPD da Asana e como os clientes podem usar a Asana para atender às suas próprias iniciativas de conformidade com esse regulamento.
- Nomeação de um responsável pela proteção de dados, com quem é possível contatar através do e-mail **dpo@asana.com**.

APPI

A Lei de Proteção das Informações Pessoais (Act on the Protection of Personal Information, APPI) é a principal lei de proteção de dados do Japão que regula a proteção das informações pessoais. Aplica-se aos operadores comerciais que processam informações pessoais de indivíduos no Japão. A Asana se compromete a processar e a proteger as informações pessoais conforme exigido pela APPI e suas emendas. O Adendo de Processamento de Dados[16] da Asana abrange (1) os nossos compromissos quanto à proteção de dados para assegurar a nossa conformidade com a APPI; (2) como forneceremos assistência aos nossos clientes em relação às suas obrigações sob a APPI; e (3) as medidas técnicas e organizacionais implementadas para proteger as informações pessoais.

Adendo de Processamento de Dados

De acordo com o RGPD, os "controladores de dados" (ou seja, as entidades que estabelecem as finalidades e meios para processamento de dados) devem celebrar um acordo com as entidades que processarem dados em seu nome (denominadas "processadores de dados"). A Asana oferece aos clientes um adendo robusto de processamento de dados ("APD") sob o qual a Asana se compromete a processar e proteger os dados pessoais de acordo com os requisitos estipulados pela legislação aplicável. Isso inclui o compromisso da Asana de processar os dados pessoais conforme as instruções do controlador de dados. O Adendo de Processamento de Dados pode ser consultado na nossa página de Termos[17] e é referenciado no contrato de assinatura aplicável entre a Asana e o cliente.

Aplicação da lei

A Asana segue as Diretrizes de solicitação de dados para a aplicação da lei descritas na nossa página de Diretrizes para a aplicação da lei.[18]

[16] https://asana.com/pt/terms#data-processing
[17] https://asana.com/pt/terms#data-processing
[18] https://asana.com/pt/terms#data-processing

Certificações, atestados e conformidade

A Asana tem o compromisso contínuo de assegurar que os seus serviços atendam aos padrões globais de segurança, privacidade e conformidade. Atualmente, a Asana mantém as seguintes certificações e atestados:

SOC 2 Tipo II: a Asana concluiu com sucesso a sua auditoria SOC 2 (Tipo II) para os controles implementados em relação à segurança, à disponibilidade e à confidencialidade. A obtenção da certificação SOC 2 (Tipo II) significa que foram estabelecidos processos e práticas sobre esses três princípios de controle que foram validados por um terceirizado independente.

ISO/IEC 27001:2013: a Asana mantém uma certificação ISO/IEC 27001:2013 que demonstra a sua conformidade com os requisitos definidos pelo padrão ISO/IEC 27001:2013 para estabelecer, implementar, manter e aprimorar continuamente o sistema de gestão da segurança da informação.

ISO 27017:2015: demonstra a conformidade da Asana com os controles de segurança da informação aplicáveis ao fornecimento e uso de serviços em nuvem.

ISO 27018:2019: demonstra as medidas implementadas pela Asana para proteger informações de identificação pessoal de acordo com os princípios de privacidade da ISO/IEC 29100 para o ambiente público de computação em nuvem.

ISO 27701:2019: demonstra o compromisso da Asana em estabelecer, manter e aprimorar continuamente um sistema de gestão da privacidade da informação como uma extensão da ISO 27001 para a gestão da privacidade na nossa organização.

Conformidade com a HIPAA

A Asana oferece proteções de segurança e privacidade que permitem aos clientes usar a Asana em conformidade com a Lei de Portabilidade e Responsabilização de Seguros de Saúde (Health Insurance Portability and Accountability Act, HIPAA) dos Estados Unidos. Os clientes que estão sujeitos à HIPAA e querem armazenar informações protegidas de saúde (Protected Health Information, PHI) na Asana devem adquirir um plano Enterprise e firmar um Acordo de empresa associada com a Asana. Para mais informações sobre conformidade com a HIPAA, entre em contato com a equipe de vendas da Asana.[19]

Registro na CSA STAR

A autoavaliação de nível 1 do Questionário da iniciativa de avaliação de consenso (Consensus Assessments Initiative Questionnaire, CAIQ) da CSA realizada pela Asana está disponível no Registro da CSA STAR.[20]

[19] https://asana.com/pt/guide/help/premium/hipaa-compliance
[20] https://cloudsecurityalliance.org/star/registry/asana-inc/services/asana/

Conclusão

Na Asana, dependemos diariamente da nossa própria plataforma para manter as equipes do mundo todo alinhadas e realizar o trabalho necessário. Mais de 100.000 outras empresas fazem o mesmo. Por isso, a nossa prioridade é manter os seus dados seguros para a tranquilidade de todos.

A Asana oferece segurança total do produto para toda a sua organização e dispõe de um programa estabelecido de conformidade e confiança para proteger os seus dados. Para saber mais sobre as ofertas dos planos pagos da Asana, entre em contato com a nossa equipe de vendas pelo e-mail sales@asana.com.

Quer reportar uma questão de segurança? Envie um e-mail para security@asana.com.