AUTODESK

Whitepaper de segurança do Autodesk® Fusion 360

Outubro de 2022

Conteúdo

1. INTRODUÇÃO 2

1.1 OBJETIVO E ESCOPO DO DOCUMENTO 2

2. SEGURANÇA DA AUTODESK 2

3. ENGENHARIA DO FUSION 360 3

3.1 TREINAMENTO DE FUNCIONÁRIOS 4

4. SEGURANÇA DO PRODUTO FUSION 360 4

4.1 SEGURANÇA DAS COMUNICAÇÕES 4
4.2 CRIPTOGRAFIA E CIFRAS 4
4.3 AUTENTICAÇÃO 4
4.4 SEGURANÇA DE DADOS 5
4.5 VERSÃO DO PROJETO 5
4.6 SEGURANÇA DA COLABORAÇÃO BASEADA EM HUB E GRUPO 5
4.7 COMPARTILHAMENTO PÚBLICO 6

5. INFRAESTRUTURA DE NUVEM 6

5.1 ALTA DISPONIBILIDADE 6
5.2 REPLICAÇÃO E REDUNDÂNCIA DE DADOS 6
5.3 REDUNDÂNCIA DO SISTEMA DE ALIMENTAÇÃO 6
5.4 REDUNDÂNCIA DE CONECTIVIDADE COM A INTERNET 6
5.5 SEGURANÇA DA INFRAESTRUTURA FÍSICA 7
5.6 CONTROLE DE ACESSO ÀS INSTALAÇÕES 7
5.7 PREVENÇÃO CONTRA INCÊNDIO 7
5.8 CONTROLES CLIMÁTICOS 7

6. GERENCIAMENTO DE INCIDENTES DE OPERAÇÕES 8

7. GERENCIAMENTO DE CORREÇÕES 8

8. GERENCIAMENTO DE ALTERAÇÕES 8

9. GERENCIAMENTO DE CAPACIDADE 9

10. ALERTAS E MONITORAMENTO 10

11. TEMPO DE INATIVIDADE ZERO DURANTE IMPLEMENTAÇÕES 10

12. CONTROLES OPERACIONAIS DO AUTODESK FUSION 360 11

13. SEGURANÇA DA AUTODESK 11

13.1 VERIFICAÇÕES DE VULNERABILIDADE E TESTES DE PENETRAÇÃO 12
13.2 SEGURANÇA DE REDE 12
13.3 CRIPTOGRAFIA 12
13.4 PRIVACIDADE 12

14. RECURSOS 13

1. Introdução

O Autodesk® Fusion 360™ é a primeira ferramenta 3D CAD, CAM e CAE do tipo. Ele conecta o processo de desenvolvimento de produtos em uma única plataforma baseada em nuvem que funciona tanto no Mac quanto no PC. As ferramentas do Fusion 360 permitem a exploração rápida e fácil de ideias de projeto com um conjunto seguro de ferramentas integradas do conceito à fabricação que se estende para incluir navegadores da Web e dispositivos móveis.

1.1 Objetivo e escopo do documento

O objetivo deste documento é explicar as operações da Autodesk, o processo de desenvolvimento de software e as medidas de segurança implementadas no ambiente. Neste documento, o Autodesk Fusion 360 se refere ao software cliente do Fusion 360 e ao software de acesso ao navegador do Fusion 360.

A estrutura de segurança da Autodesk baseia-se em padrões da indústria para proteger a confidencialidade, a integridade e a disponibilidade das informações do cliente.

O Fusion 360 foi projetado para oferecer alta disponibilidade e escalabilidade, fornecendo aos nossos clientes um serviço em nuvem rápido e resiliente. O provedor de hospedagem na nuvem da Autodesk é a AWS (Amazon Web Services), líder em infraestrutura de nuvem. A Autodesk se baseia no modelo de responsabilidade compartilhada do provedor de hospedagem AWS, que inclui a infraestrutura composta de hardware, software, rede e instalações que executam serviços na nuvem AWS. (Para obter mais informações, consulte: https://aws.amazon.com/compliance/shared-responsibility-model/).

2. Segurança da Autodesk

A estrutura de segurança da Autodesk baseia-se em padrões da indústria para garantir práticas de segurança consistentes, permitindo construir, executar e se manter em segurança.

- **Construir com segurança** - Incorporar segurança aos nossos produtos desde o início é uma parte fundamental para garantir o investimento de nossos clientes em produtos e serviços da Autodesk. Integramos a segurança em todas as fases de desenvolvimento de software.

- **Executar com segurança** - Criamos segurança diretamente em nossa infraestrutura. Nossa abordagem holística inclui a implementação de ferramentas de proteção de extremidade, requisitos padronizados de aplicação de correções e endurecimento, controles de gerenciamento de identidades e acesso e atividades de segurança ofensivas.

- **Manter-se em segurança** - A segurança na Autodesk está focada em três objetivos principais que protegem a confidencialidade, a integridade e a disponibilidade (CIA) das informações:

    - Confidencialidade: as informações são acessíveis apenas a pessoas autorizadas
    - Integridade: as informações são completas e precisas
    - Disponibilidade: os dados são acessíveis e estão disponíveis para os clientes

O Diretor de Segurança (CSO) é responsável pelo desenvolvimento, implementação e governança da estratégia e do programa de segurança e garante que as políticas e padrões de segurança sejam aplicados em todos os produtos e ambientes da Autodesk. A equipe de CSO e segurança tem suporte de executivos e do Conselho de administração da Autodesk.

3. Engenharia do Fusion 360

A equipe de engenharia do Fusion 360 é responsável por projetar, implementar e testar o aplicativo de software cliente e serviços em nuvem do Fusion 360.

O projeto, a codificação, os testes e a manutenção do Fusion 360 são baseados em um processo ágil de desenvolvimento de software. Durante as fases do projeto, os arquitetos produzem e revisam documentos de projeto detalhados para avaliar a funcionalidade e a escalabilidade do projeto. Durante as fases de implementação, os engenheiros de software e arquitetos conduzem análises de códigos de pares para detectar desvios das práticas de desenvolvimento de aplicativos do Fusion 360. Todo o código produzido durante o processo inclui teste de unidade funcional e nenhuma história de usuário é concluída até que o pessoal de controle de qualidade verifique a aceitação e a Definição de critérios de conclusão. O teste de desempenho do Fusion 360 também está integrado ao ciclo de vida de desenvolvimento. A equipe do Fusion 360 realiza testes de carga em todas as fases de desenvolvimento para identificar alterações que afetam negativamente o desempenho o mais cedo possível no processo.

3.1 Treinamento de funcionários

Todos os funcionários da Autodesk devem afirmar a importância da segurança das informações como parte da orientação a novos funcionários. Os funcionários devem ler, entender e fazer um curso de treinamento sobre o Código de Conduta da empresa. O código exige que cada funcionário realize negócios de forma legal, ética, com integridade e respeito mútuo e aos usuários, parceiros e concorrentes da empresa.

Os funcionários da Autodesk devem seguir as diretrizes da empresa em relação a confidencialidade, ética comercial, uso apropriado e padrões profissionais. Os novos funcionários devem assinar um contrato de confidencialidade. A nova orientação dos funcionários enfatiza a confidencialidade e a privacidade dos dados do cliente.

Para implementar as melhores práticas de segurança, a Autodesk introduziu um Programa de Certificação de Segurança de Software (SSCP) anual para todos os membros em funções de Engenharia e Infraestrutura de nuvem.

4. Segurança do produto Fusion 360

O Autodesk Fusion 360 tem recursos de segurança incorporados que vão desde a comunicação com os serviços em nuvem até recursos de segurança e colaboração no nível do produto que os usuários podem controlar.

4.1 Segurança das comunicações

Toda a comunicação entre o Autodesk Fusion 360 e os serviços em nuvem requer conexões HTTPS seguras.

4.2 Criptografia e cifras

A comunicação entre o Fusion 360 e os serviços de back-end e entre os serviços de back-end é feita por meio de um canal criptografado.

4.3 Autenticação

São necessárias credenciais que consistem em uma ID Autodesk, ID de usuário e senha para acessar o Autodesk Fusion 360. As credenciais são protegidas durante a transmissão de rede e armazenadas somente como um hash salgado.

O Fusion 360 oferece aos usuários finais a opção de usar a autenticação multifator ao efetuar login. Os usuários que optarem por ativar esse recurso poderão usar seu dispositivo pessoal seguro autorizado (por exemplo, telefone celular) para receber um código a ser usado em conjunto com a senha.

4.4 Segurança de dados

Todos os projetos do Fusion 360 são salvos na nuvem em armazenamento criptografado. A solução de armazenamento usa o padrão avançado de criptografia de 256 bits (AES-256) para criptografar dados.

Localmente, os projetos em cache baseiam-se nas permissões de nível de usuário do sistema operacional para o controle de acesso.

4.5 Versão do projeto

Para cada projeto, o Autodesk Fusion 360 mantém um histórico de versões. O controle de versão protege a integridade dos dados, permitindo que os usuários revertam para versões anteriores e fornecendo uma lista auditável que contém informações sobre cada modificação do arquivo.

4.6 Segurança da colaboração baseada em hub e grupo

Os projetos fornecem a um conjunto de colaboradores uma base simples para conceder ou limitar o acesso aos projetos do Autodesk Fusion 360. Os convites para projetos são aprovados pelo proprietário ou moderador do projeto, assegurando um controle rigoroso sobre os membros que concedem acesso a novos usuários.

As empresas podem optar pelos hubs de equipe, que permitem que eles exerçam a propriedade e o controle de acesso de todos os projetos criados pelos membros. As configurações de privacidade do projeto, como projetos abertos, fechados e secretos, permitem colaboração controlada. Com os hubs da equipe, os membros podem optar por restringir o acesso aos colaboradores que foram convidados para o projeto. Os hubs da equipe também permitem que os administradores do cliente desativem contas de ex-funcionários e transfiram a propriedade do projeto para outros membros da equipe.

4.7 Compartilhamento público

Com o compartilhamento público, os usuários podem colaborar com outros envolvidos que não têm ID Autodesk ou direito ao Fusion 360. Os usuários do Fusion 360 criam um link que fornece acesso somente leitura ao projeto. Os usuários também têm a opção de ativar os recursos de download/exportação. A qualquer momento, o usuário pode revogar o compartilhamento público oferecido por este link.

5. Infraestrutura de nuvem

A equipe de infraestrutura de nuvem é responsável por definir e executar procedimentos para gerenciamento de versões de aplicativos, atualizações de hardware e sistema operacional, monitoramento de integridade do sistema e outras atividades necessárias para manter o Autodesk Fusion 360.

5.1 Alta disponibilidade

O Autodesk Fusion 360 foi projetado para alcançar um alto nível de disponibilidade, empregando sistemas redundantes em sua infraestrutura de suporte e distribuindo a carga em uma frota de instâncias escalável.

5.2 Replicação e redundância de dados

A replicação dos dados do cliente é realizada entre as zonas de disponibilidade (AZs) da AWS (Amazon Web Services). A replicação limitará a possibilidade de perda de dados ou de atraso na retomada do serviço se for necessário realizar failover em um data center de backup.

5.3 Redundância do sistema de alimentação

Os data centers AWS contêm sistemas de energia elétrica redundantes para manter as operações 24 horas por dia, sete dias por semana. As fontes de alimentação ininterrupta fornecem automaticamente backup para os sistemas elétricos principais em caso de falha. Os geradores em cada data center fornecerão alimentação de backup de longo prazo caso ocorra uma interrupção.

5.4 Redundância de conectividade com a Internet

Um sistema redundante de vários fornecedores é usado para manter a conectividade com a Internet em cada um dos data centers.

O software cliente do Autodesk Fusion 360 também tem um modo off-line para permitir que os usuários continuem acessando e trabalhando em cópias locais de seus projetos quando não estão conectados à Internet.

5.5 Segurança da infraestrutura física

O aplicativo Autodesk Fusion 360 é executado em data centers seguros AWS que são protegidos contra acesso físico não autorizado e riscos ambientais por uma variedade de controles de segurança. Alguns controles físicos e ambientais estão resumidos abaixo. Uma visão geral completa dos processos de segurança da AWS está disponível aqui.

5.6 Controle de acesso às instalações

Os data centers AWS são protegidos 24 horas por dia, 7 dias por semana por equipes profissionais de segurança física. Os perímetros de cada data center, bem como os ambientes que contêm equipamentos de computação e suporte, são protegidos por vigilância por vídeo. A vigilância por vídeo é preservada na mídia digital, o que permite que atividades recentes sejam visualizadas sob demanda. As entradas do data center são protegidas por armadilhas que restringem o acesso a uma única pessoa de cada vez. Todos os visitantes e prestadores de serviços devem apresentar identificação para serem admitidos e são acompanhados por pessoal autorizado em todos os momentos. Somente funcionários com necessidades comerciais legítimas recebem acesso ao data center; e todas as visitas são registradas eletronicamente.

5.7 Prevenção contra incêndio

Sistemas de detecção e supressão de incêndios, como alarmes de fumaça e tubulações úmidas ativadas por calor, são instalados em cada data center para proteger ambientes que contêm equipamentos de computação e sistemas de suporte. Os sensores de detecção de incêndio são instalados no forro e abaixo de um piso elevado.

5.8 Controles climáticos

Os controles climáticos do data center protegerão servidores, roteadores e outros equipamentos sujeitos a falhas se forem violadas faixas ambientais rigorosas. O monitoramento por parte dos sistemas e do pessoal está em vigor para evitar que ocorram condições perigosas, como sobreaquecimento. Ajustes que mantêm a temperatura e outras medidas ambientais dentro de faixas aceitáveis são feitos automaticamente por sistemas de controle.

6. Gerenciamento de incidentes de operações

A Autodesk tem uma política de gerenciamento de incidentes que define as melhores práticas para orientar a resolução de incidentes. A política de gerenciamento de incidentes da Autodesk enfatiza o registro de etapas de correção e o uso de análise de causa raiz para criar uma base de conhecimento de procedimentos acionáveis. A meta da política de gerenciamento de incidentes da Autodesk não é apenas fechar incidentes de forma rápida e eficaz, mas também coletar e distribuir informações sobre incidentes para que os processos sejam continuamente aprimorados e as respostas futuras sejam direcionadas por conhecimento acumulado.

7. Gerenciamento de correções

A equipe de infraestrutura de nuvem tem uma política de gerenciamento de correções que ajuda a garantir uma implementação de correções eficaz. Quando possível, a automação está em vigor para verificar novas correções e preparar listas de implementação que podem ser aprovadas por pessoal autorizado da infraestrutura de nuvem. A política de aplicação de correções também define critérios para determinar o impacto de uma correção na estabilidade do sistema. Se uma correção for identificada como de possível alto impacto, o teste de regressão será concluído antes que a correção seja implementada. O Gerenciamento de alterações rastreia a implementação de correções em sistemas de produção.

8. Gerenciamento de alterações

A equipe de infraestrutura de nuvem tem uma política de gerenciamento de alterações que inclui as seguintes atividades:

- **Pedido de alteração (RFC).** Um formulário de RFC deve ser enviado para todas as alterações. O formulário inclui o nome do iniciador da alteração, a prioridade da alteração, a justificativa de negócios para a alteração e uma data de implementação de alteração solicitada.

- **Planos de retrocesso.** A equipe de infraestrutura de nuvem cria planos detalhados de retrocesso antes da implementação, para que o estado do sistema possa ser restaurado se uma alteração causar uma interrupção do serviço. Os planos de retrocesso incluem

instruções executáveis definidas em scripts que restauram o estado do sistema com um mínimo de etapas manuais.

- **Janelas de manutenção definidas.** A equipe de infraestrutura de nuvem especifica janelas de manutenção programadas, emergenciais e estendidas. Eles programam uma manutenção planejada fora dos horários de pico.

- **Plano de teste.** A equipe de infraestrutura de nuvem define um conjunto de testes para verificar se a funcionalidade está acessível após a implementação de uma alteração.

- **Execução de testes.** Quando a implementação é concluída, a equipe de CQ do Autodesk Fusion 360 e da infraestrutura de nuvem executará os testes para verificar se a funcionalidade identificada como em risco permanece disponível.

9. Gerenciamento de capacidade

Como o acesso do cliente aos serviços em nuvem é provisionado sob demanda por meio de um modelo de autoatendimento, os padrões de tráfego são altamente variáveis e estão sujeitos a picos de uso. Quando ocorre um pico, a disponibilidade de um serviço poderá ser afetada negativamente se o pool de recursos de computação que alimenta o serviço estiver esgotado. Para manter um alto nível de disponibilidade, a equipe de infraestrutura de nuvem implementa uma política de gerenciamento de capacidade. Essas práticas incluem:

- **Gravação frequente do uso de recursos.** O uso de recursos do Autodesk Fusion 360 é coletado em intervalos frequentes em uma variedade de componentes de infraestrutura, incluindo instâncias virtuais, volumes de armazenamento virtual e dispositivos de rede virtual. As estatísticas de uso são armazenadas em um repositório de gerenciamento de capacidade.

- **Planejamento de capacidade.** A equipe de infraestrutura de nuvem usa o gerenciamento de capacidade para gerar um plano detalhado de capacidade que documenta os níveis atuais de uso e modela níveis futuros com base na análise estatística e no impacto dos aprimoramentos futuros na funcionalidade dos negócios. O

plano de capacidade será atualizado conforme necessário ou se alterações significativas nos padrões de uso forem detectadas.

- **Alocação de recursos.** Os recursos computacionais são alocados conforme os clientes os solicitam. Os recursos de cálculo pré-aquecidos estão sempre disponíveis. Se ocorrer um aumento de atividade, novos recursos serão instanciados. Por exemplo, a disponibilidade dos recursos do navegador do Autodesk Fusion é geralmente obtida em menos de 10 minutos.
- **Monitoramento de atividades.** Os painéis de atividades e alertas são definidos nos serviços de back-end, permitindo que os engenheiros observem a atividade do sistema e executem exames e análises pós-incidentes.

10. Alertas e monitoramento

Para fornecer o menor Tempo médio até a correção possível, a Autodesk usa sistemas automatizados para monitorar o Fusion 360, validando o estado de integridade do serviço. Cada componente único, do banco de dados aos serviços, é monitorado individualmente.

No caso de um evento que afeta o serviço, são gerados alertas, e a equipe de infraestrutura de nuvem é notificada por meio de um processo de escalonamento.

A integridade do serviço também descreve a relação entre os serviços da Autodesk. Um serviço como o Autodesk Fusion 360 é altamente sensível ao serviço ACM (Controle de acesso). Cada serviço deverá ser resiliente quando um serviço dependente falhar e deverá falhar suavemente quando não puder mais operar sem perda de dados para o cliente.

O estado do serviço do Fusion 360 é exibido publicamente pelo Serviço do Health Dashboard da Autodesk: https://health.autodesk.com.

11. Tempo de inatividade zero durante implementações

À medida que são aplicadas correções ao ambiente de produção, uma abordagem de implementação azul-verde é usada para o navegador do Autodesk Fusion e outros serviços do Fusion 360. Isso ajuda a garantir que os clientes não tenham tempo de inatividade do serviço.

12. Controles operacionais do Autodesk Fusion 360

O Autodesk Fusion 360 fornece proteção de dados confidenciais de clientes contra acesso não autorizado.

- **Restrições físicas aos data centers.** As restrições físicas aos data centers impedem que pessoas não autorizadas acessem o hardware e os sistemas de suporte usados pelo Autodesk Fusion 360.
- **Verificações em segundo plano.** As verificações em segundo plano são necessárias para os funcionários com acesso físico aos recursos de computação e sistemas de suporte usados pelo Autodesk Fusion 360.
- **Replicação de dados.** A replicação de dados copia os dados do cliente em data centers redundantes para que a continuidade de negócios possa ser mantida se ocorrer um failover entre as instalações.
- **Tecnologias redundantes**. Tecnologias redundantes, como balanceadores de carga e bancos de dados agrupados, limitam pontos únicos de falha.

13. Segurança da Autodesk

A equipe de segurança da Autodesk é um grupo dedicado de especialistas em segurança de informações focados na identificação e na aplicação de práticas de segurança no ambiente de nuvem da Autodesk. As responsabilidades da equipe de segurança da Autodesk incluem:

- Análise da postura de segurança do projeto e da implementação da infraestrutura de nuvem da Autodesk.
- Definição e garantia da implementação de políticas de segurança, incluindo gerenciamento de identidades e acesso, gerenciamento de senhas e gerenciamento de vulnerabilidades.
- Impulsionamento da conformidade com os procedimentos de segurança estabelecidos por meio de revisões e auditorias internas.

- Identificação de implementação de tecnologias que protejam as informações do cliente
- Envolvimento de especialistas em segurança de terceiros para realizar avaliações de segurança das informações
- Monitoramento dos serviços em nuvem quanto a possíveis problemas de segurança e resposta a incidentes conforme necessário
- Realização de revisões anuais da política de segurança da Autodesk.

13.1 Verificações de vulnerabilidade e testes de penetração

Os serviços do Fusion 360 são submetidos a um teste de penetração anual e a verificações regulares de ameaças e vulnerabilidades de segurança. O aplicativo também sofre análise estática e verificações de bibliotecas de terceiros. As verificações de segurança e os testes de penetração abrangem uma ampla gama de vulnerabilidades definidas pelo Open Web Application Security Project (OWASP) e pelo SANS top 25.

13.2 Segurança de rede

A segurança de rede é aplicada usando uma combinação de controles físicos e lógicos, incluindo criptografia, firewalls e procedimentos de endurecimento de sistemas. Além disso, a AWS fornece controles de segurança de rede que protegem seus data centers físicos. Para obter mais informações, consulte as Práticas recomendadas de segurança, identidade e conformidade.

13.3 Criptografia

Todo o tráfego de rede é criptografado quando transmitido pela Internet para o perímetro do ambiente de nuvem da Autodesk. Informações confidenciais, como credenciais, informações de sessão do aplicativo, tokens de acesso e perfis de usuário, são criptografadas quando inativas.

13.4 Privacidade

A Autodesk é transparente sobre como os dados pessoais dos clientes são coletados e usados. Leia a Declaração de privacidade da Autodesk para saber mais.

14. Recursos

Os recursos a seguir fornecem informações gerais sobre a Autodesk e outros tópicos mencionados na seção principal deste documento.

- **Autodesk** - Para visualizar informações sobre a Autodesk, visite https://www.autodesk.com.br.
- **Autodesk Trust Center** - Para visualizar informações sobre o Autodesk Trust Center, visite http://trust.autodesk.com.
- **Autodesk Fusion 360** - Para visualizar informações sobre o Fusion 360, visite http://fusion360.autodesk.com.