www.mcfile.com

1. Breve descrição

McFile é um Software as a Service (SaaS) para gerenciamento de informações e dados empresariais. A solução é totalmente hospedada na nuvem, utilizando majoritariamente a AWS (Amazon Web Services) e serviços pontuais da GCP (Google Cloud Plataform).

Por ser em nuvem, o McFile é escalável, elástico e possui alta disponibilidade em seus serviços.

2. Acesso ao sistema

I. Acesso por usuário

Os usuários podem acessar o sistema de diferentes maneiras

- Browsers: Pode ser acessado normalmente pelas versões mais atuais dos browsers utilizados no mercado, Chrome, Firefox, Edge, IE e Safari.

- Aplicativos: Disponíveis na App Store (iPhone, iPad) e na Google Play (Android). Através deles é possível pesquisar, cadastrar, consultar e compartilhar documentos e informações contidas no sistema.

- McOffice (Plug-in Office): Facilita o cadastro e edição de documentos diretamente pela suíte Office (Word, Excel, Powerpoint e Outlook).

II. Acesso por sistemas / Integração

O McFile possui Web Services disponíveis para que sejam desenvolvidas integrações com seus dados. Essas chamadas seguem o modelo REST e devem ser feitas por HTTP POST.

Também é possível a realização de integração utilizando a aplicação em Java McIntegrador, disponível no GitHub publicamente. Ela faz uso dos Web Services descritos acima e pode acessar os dados localmente, de um banco de dados ou arquivos TXT, por exemplo.

Outra possibilidade de integração é a utilização de um “Widget”, uma biblioteca Javascript que pode ser adicionada numa aplicação web para comunicação com o McFile. Ela possui funções de inserção, pesquisa e visualização de documentos.

Todo ambiente também possui um webhook de inserção de e-mails. Ao criar uma conta no McFile, é criado automaticamente uma caixa de entrada cliente@mcfile.com, que pode ser utilizada para, facilmente, enviar arquivos para o sistema.

Esses e-mails podem ser categorizados manualmente através do uso de hashtag (#) ou pela McOffice através de tokens de referência ([Ref. XXXXXX]) no assunto do e-mail.

3. Segurança de acesso

Os dados em trânsito são protegidos através do protocolo HTTPS, com certificado TLS 1.3.

Para acessar o McFile é necessário inserir login e senha válidos. Um usuário tem seu acesso e permissão controlados por uma tela de gestão de usuários, onde é possível alterar privilégios, áreas de sigilo, além de bloquear acessos e cadastrar novos usuários.

As áreas de sigilo funcionam como cofres no sistema, documentos criados em uma área só podem ser visualizados e acessados por pessoas que tenham acesso à mesma (de edição ou visualização).

Sistema é protegido por tecnologia CAPTCHA, para bloquear tentativas de acesso por agentes mal-intencionados.

As chamadas de integração também são autenticadas, utilizando chave de integração, que pode ser de dois tipos: por usuário ou global.

O acesso de cada usuário também pode ser configurado com regras de IP, bloqueando logins que não respeitem IPs previamente cadastrados. Assim, pode-se controlar de onde usuários selecionados utilizam a ferramenta.

Sistema está habilitado para integrações através de protocolo OAuth 2.0 e OpenID Connect.

4. Gerenciamento dos dados e arquivos

I. Localização

Todos os dados armazenados no McFile são mantidos em servidores e serviços na região de São Paulo.

II. Arquivos

Os arquivos no McFile são armazenados na solução Amazon S3 (Simple Storage Service). Eles são replicados em vários servidores separados geograficamente, de forma que estão protegidos contra qualquer ação mal-intencionada ou pane no sistema. Além disso, os arquivos são armazenados criptografados utilizando padrão AES-256.

Todos os acessos à arquivos são feitos através de API protegida por criptografia e chaves de acesso.

Para exclusão definitiva de um arquivo é necessário procedimento especial de aprovação em duas camadas, com o fornecimento de código de autenticação MFA (Multi-Factor Authentication).

Para mais informações sobre o S3, veja: https://aws.amazon.com/s3/

III. Banco de dados

O banco de dados utiliza o Amazon RDS (Relational Database Service), e é mantido em última versão de patches através de atualizações periódicas.

Os dados são criptografados em trânsito e em repouso, através de padrão de mercado AES-256.

Para mais informações sobre o RDS: https://aws.amazon.com/rds/

IV. Backup

Além da replicação automática de arquivos, o sistema possui mais duas políticas de backup.

Banco de dados: backup ocorre a cada 15 minutos e é retido por uma semana. Snapshots completas são criadas diariamente.

Índice de pesquisa (utilizado pelo módulo de pesquisa): backup ocorre diariamente e é retido por um mês. Pode ser gerado novamente pelo banco de dados

Os backups são armazenados criptografados no S3, também possuindo redundância em diferentes servidores.

V. Auditoria

Toda a atividade dos usuários do serviço é monitorada e registrada em logs de auditoria.

Administradores e gestores podem gerar relatórios completos com todo o histórico de um usuário e/ou arquivo.

VI. Garantias

Os dados dos clientes são protegidos por NDA (Non-disclosure agreement) entre as partes. Além disso, não são trafegados para fora do ambiente Amazon pela equipe de suporte McFile.

Em caso de término de contrato, os dados são devolvidos ao cliente em estrutura de pastas e posteriormente destruídos, conforme definido em contrato.

A destruição de dados é feita através de desativação de mídias utilizando padrão de mercado NIST 800-88.

5. Gestão de infraestrutura

I. Monitoramento e auditoria

Todo o ambiente em nuvem é monitorado continuamente para garantir performance, segurança e auditoria.

Monitoramento é feito através de serviços contra atividades mal-intencionadas, comportamentos não autorizados e health checks que validam disponibilidade e tempo de resposta dos serviços.

Entre as atividades mal-intencionadas, podemos destacar: ataques DDoS, comprometimento de credenciais, chamadas de API provenientes de IPs mal-intencionados conhecidos, entre outras.

Para mais informações sobre alguns serviços utilizados, podem ser consultados os dois sites abaixo:
- https://aws.amazon.com/shield/
- https://aws.amazon.com/guardduty/

Além disso, qualquer ação é registrada em logs de auditoria que podem ser analisados e compilados em caso de necessidade.

II. Patches e atualizações

Banco de dados, sistemas operacionais e ferramentas são periodicamente atualizados com último patch disponível.

Mudanças maiores, como versões de sistema operacional ou engine de banco de dados, são agendadas com antecedência, informadas aos clientes caso haja algum impacto e efetuadas por equipe especializada.

III. Política de Disaster Recovery

Em caso de interrupção do servidor primário, é acionado servidor de contingência através de tecnologia AMI (Amazon Machine Images), que possibilita a criação de uma imagem de máquina. Essa imagem pode então ser utilizada para criar servidores sempre que necessário.

A política possui os seguintes parâmetros:

- RTO (Recovery time objective): de 2 a 4 horas úteis, dependendo do tempo de propagação do DNS

- RPO (Recovery point objective): Banco de dados é recuperado a seu estado de até 15 minutos antes do sinistro ter ocorrido. Arquivos são conservados de acordo com premissa S3. Índice do dia anterior é recuperado e registros mais recentes são reindexados.

IV. Compliance e ISO

Servidores e serviços de fornecedores em nuvem operam com standards de qualidade padrão ISO 27001, padrão para sistemas de gestão da segurança da informação (ISMS – Informations Security Management System).

Professionais da Destaque Gestão Documental recebem treinamento periódico sobre práticas de segurança e comprometimento com os dados que gerenciam.

Destaque também segue procedimentos e normas definidos pelas ISO 9001:2015, ISO 27001:2013 e 27018:2018.

6. Histórico das alterações

DATA	REVISÃO	HISTÓRICO
01/10/2020	01	Versão inicial