mcfile.com

1. Breve descrição

McFile é um software no modelo Software as a Service (SaaS) para gerenciamento de informações e dados empresariais.

A solução é totalmente hospedada na nuvem, operando sobre provedores globais de alta disponibilidade e segurança, com infraestrutura escalável e certificações internacionais.

Por ser uma solução em nuvem, a McFile é escalável, elástica e apresenta alta disponibilidade em seus serviços.

2. Acesso ao sistema

2.1. Acesso por usuário

Os usuários podem acessar o sistema de diferentes maneiras.

Navegadores

Acesso compatível com as versões mais recentes dos principais navegadores do mercado, como o Google Chrome e Microsoft Edge.

Aplicativos móveis

Disponíveis na App Store (iPhone, iPad) e Google Play (Android). Permitem pesquisar, cadastrar, consultar e compartilhar documentos e informações do sistema.

McFile for Office / McOffice

Facilita o cadastro e a edição de documentos diretamente a partir da suíte Microsoft Office (Word, Excel, PowerPoint e Outlook).

2.2. Acesso por sistemas / Integração

O McFile disponibiliza APIs RESTful para desenvolvimento de integrações com seus dados e serviços. A documentação completa da API está disponível em: apidocs.mcfile.com.

Também é possível integrar por meio da aplicação **McIntegrador** ou **McFile Integration Engine** (MIE).

Esses métodos utilizam a API mencionada e podem acessar dados locais, de um banco de dados ou arquivos TXT, por exemplo.

Outra alternativa é o uso do **McFile Widget**, uma biblioteca JavaScript que pode ser incorporada a aplicações web, oferecendo funções de inserção, pesquisa e visualização de documentos.

Cada ambiente possui ainda um webhook para inserção de e-mails. Ao criar uma conta, é gerado automaticamente um endereço ambiente@mcfile.com, que pode ser usado para envio direto de arquivos ao sistema.

E-mails podem ser categorizados manualmente com hashtags (#) ou automaticamente via McOffice, utilizando tokens de referência no assunto (por exemplo, [Ref. XXXXXX]).

3. Segurança de acesso

Os dados em trânsito são protegidos por criptografia TLS 1.3 sobre o protocolo HTTPS.

O acesso ao McFile requer login e senha válidos, com controle individual de permissões. A gestão de usuários permite alterar privilégios, definir áreas de sigilo, bloquear acessos e cadastrar novos usuários.

As áreas de sigilo funcionam como cofres de segurança: registros e documentos criados em uma área só podem ser visualizados por pessoas com acesso à mesma.

O sistema é protegido por uma camada de segurança de aplicação (WAF) que aplica regras OWASP, bloqueia entradas maliciosas e IPs suspeitos, previne injeções de código ou SQL, e utiliza CAPTCHA e rate limiting para mitigar ataques automatizados.

Também é possível restringir acessos por regras de IP, bloqueando logins não provenientes de endereços previamente cadastrados.

O McFile é compatível com os padrões OAuth 2.0 e OpenID Connect, permitindo integração segura com provedores de identidade.

4. Gerenciamento dos dados e arquivos

4.1. Localização

Todos os dados da McFile são armazenados em servidores e serviços na região de São Paulo (Brasil).

4.2. Arquivos

Os arquivos são armazenados na solução Amazon S3 (Simple Storage Service), replicados em múltiplos servidores geograficamente distribuídos, garantindo resiliência e alta disponibilidade.

Os dados são criptografados em repouso utilizando o padrão AES-256, e todo acesso é feito por API protegida com autenticação e criptografia.

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).

4.3. Banco de dados

O banco de dados utiliza o Amazon RDS (Relational Database Service), mantido com os patches mais recentes por meio de atualizações periódicas.

Os dados são criptografados em trânsito e em repouso, seguindo padrões de mercado.

4.4. Backup

Além da replicação automática, o sistema adota duas políticas complementares de backup:

- **Banco de dados**

Backups automáticos a cada 15 minutos, retidos por sete dias. Snapshots completas diárias.

- **Índice de pesquisa**

Backups diários, retidos por sete dias. O índice pode ser restaurado a partir do banco de dados.

Todos os backups são armazenados criptografados no S3, com redundância em múltiplas zonas de disponibilidade.

4.5. Auditoria

Todas as ações de usuários e administradores são registradas em logs de auditoria.

Relatórios detalhados podem ser gerados com histórico completo por data, usuário, registro ou arquivo.

4.6. Garantias

Os dados dos clientes são protegidos por acordos de confidencialidade (NDA) entre as partes e não são transferidos para fora do ambiente AWS pela equipe McFile.

Em caso de encerramento contratual, os dados são devolvidos ao cliente em estrutura de pastas e, posteriormente, destruídos de forma segura, conforme a norma NIST 800-88 (desativação de mídias).

5. Gestão de infraestrutura

5.1. Monitoramento e auditoria

O ambiente em nuvem é monitorado continuamente para garantir desempenho, disponibilidade e segurança.

São utilizados serviços de detecção de atividades maliciosas, verificação de integridade, health checks e análise de logs.

Entre as ameaças monitoradas estão ataques DDoS, comprometimento de credenciais e acessos suspeitos via API.

Ferramentas como AWS Shield e AWS GuardDuty são empregadas para proteção ativa e alertas automatizados.

Todos os eventos são registrados em logs centralizados, analisáveis pelo time técnico.

5.2. Ferramentas de análise de vulnerabilidades

São realizadas varreduras periódicas de vulnerabilidades em servidores e aplicações, com uso de ferramentas automatizadas.

Essas análises identificam e classificam riscos, como configurações inseguras, bibliotecas desatualizadas e falhas conhecidas, permitindo ações proativas de correção.

5.3. Patches e atualizações

Todos os componentes de infraestrutura, bancos de dados, sistemas operacionais e aplicações, são atualizados periodicamente com os últimos patches de segurança.

Mudanças maiores (como atualização de engine de banco ou sistema operacional) são planejadas e comunicadas previamente aos clientes caso causem algum impacto no sistema.

5.4. Política de Disaster Recovery

Em caso de indisponibilidade de servidor primário, um servidor de contingência é ativado a partir de uma imagem, permitindo rápida restauração do ambiente.

A política possui os seguintes parâmetros:

- **RTO (Recovery time objective)**: de 2 a 4 horas úteis
- **RPO (Recovery point objective)**: até 15 minutos de perda máxima de dados

Os arquivos permanecem íntegros durante o processo, pois são armazenados de forma redundante em múltiplas zonas de disponibilidade, garantindo alta disponibilidade e resiliência.

Os índices de pesquisa são restaurados a partir do backup mais recente, e os registros são reindexados conforme necessário.

5.5. Conformidade e padrões internacionais

Os serviços e fornecedores em nuvem da McFile seguem padrões internacionais de gestão e segurança da informação.

A Destaque Gestão Documental adota práticas e controles baseados nas normas ISO 9001, ISO 27001, e ISO 27018.

Sua equipe recebe treinamentos periódicos em segurança da informação, confidencialidade e conformidade com a LGPD.

O modelo de segurança também segue o princípio de responsabilidade compartilhada na nuvem, ver Seção 6.

6. Segurança compartilhada e boas práticas do cliente

A segurança da McFile é baseada em um modelo de responsabilidade compartilhada, no qual tanto a plataforma quanto seus usuários têm papéis essenciais na proteção das informações.

Enquanto a McFile garante a segurança da infraestrutura, aplicações e dados em nuvem, cabe ao cliente e aos usuários finais adotarem boas práticas no uso da solução para manter o ambiente protegido.

6.1. Proteção de credenciais

Os usuários são responsáveis por manter suas credenciais de acesso seguras, evitando o compartilhamento de logins e senhas.

Recomenda-se o uso de autenticação multifator (MFA), senhas fortes e exclusivas, e a alteração periódica dessas credenciais.

A equipe administrativa deve monitorar e revogar acessos de ex-colaboradores imediatamente após o desligamento.

6.2. Gestão de permissões e sigilo

A McFile oferece perfis de acesso e áreas de sigilo para controle granular das informações. Os administradores devem garantir que cada usuário possua apenas os privilégios necessários

(princípio do menor privilégio) e que documentos sensíveis sejam armazenados nas áreas de sigilo apropriadas.

A revisão periódica das permissões e das áreas de acesso é essencial para manter o ambiente seguro e em conformidade.

6.3. Integração com login corporativo

Sempre que possível, recomenda-se a integração com provedores de identidade corporativa (Single Sign On via OAuth 2.0 e OpenID Connect).

Essa prática centraliza a autenticação, facilita a aplicação de políticas de segurança organizacionais (como MFA e bloqueio por IP) e reduz o risco de uso indevido de credenciais individuais.

6.4. Armazenamento e compartilhamento de documentos

Os usuários devem utilizar os recursos de compartilhamento seguro oferecidos pela plataforma, evitando o envio de arquivos por canais externos ou não criptografados.

Documentos confidenciais devem permanecer sempre em áreas restritas, com controle de visualização e download.

6.5. Boas práticas de uso

- Bloquear o computador ou dispositivo sempre que se ausentar.
- Não reutilizar senhas corporativas em outros sistemas.
- Evitar acessar a McFile em redes Wi-Fi públicas ou não seguras.
- Utilizar antivírus e sistemas atualizados em todos os dispositivos de acesso.
- Notificar o administrador do sistema caso perceba comportamentos suspeitos ou acessos indevidos.

6.6. Revisão contínua

A segurança da informação depende de atualização constante das práticas de uso.

A McFile recomenda que as empresas realizem revisões periódicas de acessos, permissões e áreas de sigilo, além de treinamentos periódicos sobre boas práticas de segurança e confidencialidade.

7. Histórico das alterações

DATA	REVISÃO	HISTÓRICO
01/10/2020	01	Versão inicial
23/02/2026	02	Revisão geral: atualização de normas ISO, inclusão de varredura de vulnerabilidades, testes de DR, seção de segurança compartilhada e ajustes

		técnicos / redação.