



A segurança está
garantida,
trabalhe com toda
a tranquilidade



speechi
connect

Bem-vindo ao Speechi Connect, a nossa plataforma SAAS, onde a segurança e a fiabilidade estão no centro das nossas soluções.

Descubra os elementos técnicos e de segurança que fazem da nossa solução uma escolha segura e eficaz, independentemente da sua utilização.



AUTENTICAÇÃO

A plataforma utiliza IAM para uma autenticação segura e simplificada, integrando reconhecimento biométrico e gestão de múltiplos fatores, estando em conformidade com as normas internacionais e reduzindo os riscos de segurança.



ARMAZENAMENTO

O serviço oferece armazenamento temporário e seguro, garantindo trocas de dados encriptadas sem persistência de informações, em conformidade com as normas internacionais de segurança, com servidores localizados na Europa e eliminação automática dos dados no final de cada sessão



INFRAESTRUTURA

O sistema está protegido por um firewall aplicativo avançado, uma segmentação rigorosa da infraestrutura, auditorias de segurança regulares e monitorização contínua, garantindo uma proteção ideal contra ameaças e conformidade com as normas internacionais de segurança.

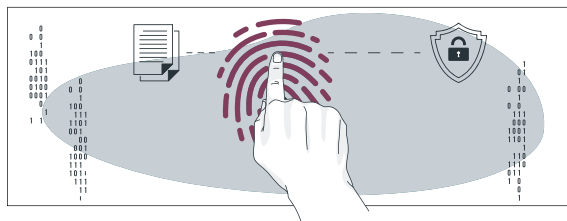
AUTENTICAÇÃO

A nossa plataforma Speechi Connect utiliza IAM (Gestão de Identidade e Acesso) para a autenticação dos utilizadores, garantindo assim um elevado nível de segurança e fiabilidade. A Speechi não tem acesso aos seus identificadores nem às suas palavras-passe. O serviço IAM Cloud oferece várias vantagens.



Conexão simplificada

Compatível com os principais fornecedores de identidade, como **Google e Microsoft**.



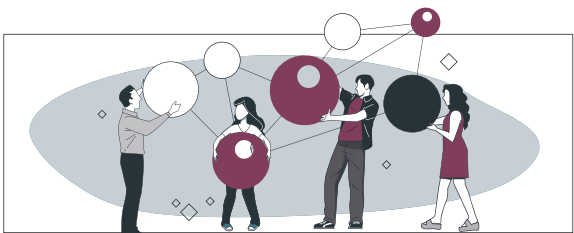
Reconhecimento biométrico

Integração de **reconhecimento biométrico** para maior segurança e uma experiência de utilizador aprimorada



Gestão multi-fatores (MFA)

Possibilidade de **autenticação dupla** para uma proteção reforçada.



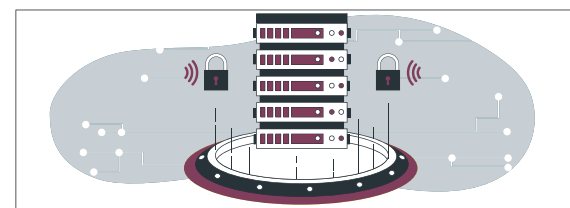
Escalabilidade

Suporta milhões de utilizadores sem comprometer o desempenho.



Conformidade e segurança

Certificado conforme as normas internacionais de segurança, incluindo **RGPD e HIPAA**.



Redução de riscos

Com base num fornecedor especializado e reconhecido mundialmente, os riscos de segurança relacionados com a gestão interna de identificadores e acessos são controlados e minimizados.

ARMAZENAMENTO

Armazenamento temporário seguro

O Speechi Connect oferece um armazenamento temporário para facilitar a troca segura entre os seus dispositivos e os ecrãs interativos. As vantagens deste sistema são múltiplas.



Trocas seguras

Os dados são transferidos de forma segura, sem deixar vestígios nos servidores.



Dados não persistentes

Nenhum dado é mantido após a utilização, minimizando os riscos de fugas ou acessos não autorizados.



Encriptação SSE por defeito

A encriptação SSE no lado do servidor destina-se a proteger os dados. Os objetos são encriptados de acordo com a norma SSE-S3 (Encriptação no Lado do Servidor com Chaves Geridas pelo S3) com chaves de encriptação geridas pelo servidor de armazenamento.



Encriptação na transferência de dados

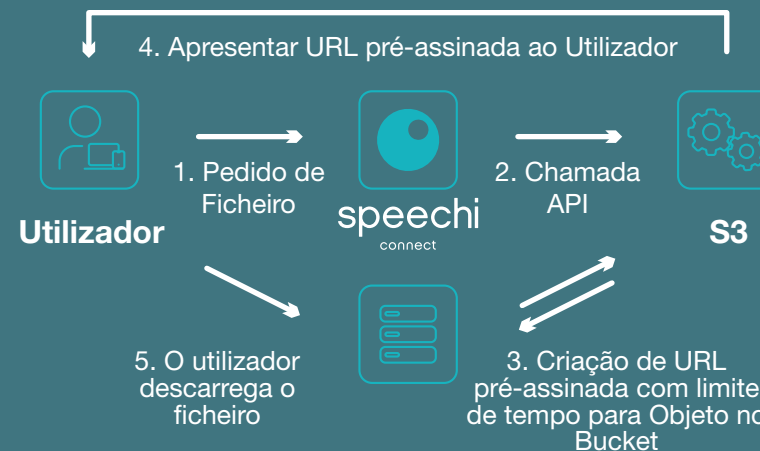
Para proteger os dados durante a transferência, os dados são encriptados utilizando Transport Layer Security (TLS 1.3).



Certificação e conformidade

Os nossos servidores de armazenamento têm várias certificações de segurança e conformidade, incluindo PCI-DSS, HIPAA/HITECH, FedRAMP, SEC Rule 17-a-4, FISMA, e cumprem a diretiva europeia de proteção de dados.

Ausência de acesso direto a armazenamentos pessoais e profissionais



A nossa plataforma foi concebida para proteger a sua privacidade e os seus dados mais sensíveis. Assim, garantimos que não há acesso direto aos ambientes de armazenamento profissionais ou pessoais dos utilizadores. Esta separação rigorosa protege as suas informações contra qualquer tentativa de intrusão ou exploração.

Nenhum ficheiro passa pelo nosso back office, seja durante a transferência de dados dos seus dispositivos para o ecrã interativo, durante a recuperação do seu trabalho, ou do ecrã interativo para os seus dispositivos.

Utilizamos um sistema de URLs pré-assinadas e os fluxos são encriptados com TLS 1.3.



Confirmidade com as normas Europeias para armazenamento

Comprometemo-nos a respeitar as rigorosas regulamentações Europeias em matéria de proteção de dados.

Os nossos servidores SAAS estão localizados na Europa, mais especificamente na Irlanda, na França e na Alemanha, garantindo:

- Uma **total conformidade com o RGPD** e o cumprimento das diretivas da União Europeia em matéria de proteção de dados.
- Um alto nível de desempenho e disponibilidade graças a uma infraestrutura robusta e escalável.

Note-se que um **CDN (Rede de Distribuição de Conteúdo)** está nativamente integrada na nossa plataforma, de modo que, quando um utilizador solicita conteúdo, a CDN redireciona esse pedido para o servidor mais próximo do utilizador, minimizando assim o tempo de latência.



Criptografia dos dados

A segurança dos dados armazenados na nossa plataforma é garantida por mecanismos de criptografia avançados:

- **Criptografia SSE-KMS** (Criptografia do Lado do Servidor com Key Management Service): todos os dados armazenados são encriptados e legíveis através de uma chave de criptografia única. Os dados são ilegíveis sem esta chave de criptografia.
- Gestão de chaves: **as chaves de criptografia são protegidas** através de um sistema de gestão de chaves independente.
- Transporte seguro: os dados são transmitidos através de **protocolos seguros (TLS/SSL)** para impedir intercepções.



Eliminação de dados no final da sessão

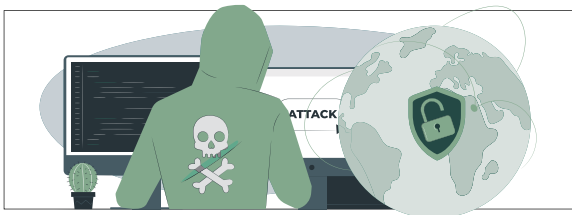
Garantimos a confidencialidade e a segurança das suas atividades ao eliminar todos os vestígios da sua sessão quando sai do ecrã interativo:

- **Eliminação de notas:** todas as notas elaboradas no ecrã interativo são automaticamente eliminadas ao final da sessão de trabalho.
- **Histórico de navegação:** o histórico de navegação na internet, assim como os logins e palavras-passe eventualmente introduzidos durante a sessão, são automaticamente eliminados.
- **Ficheiros descarregados:** os ficheiros descarregados também são eliminados no final da sessão para evitar qualquer retenção indesejada.

INFRAESTRUTURA

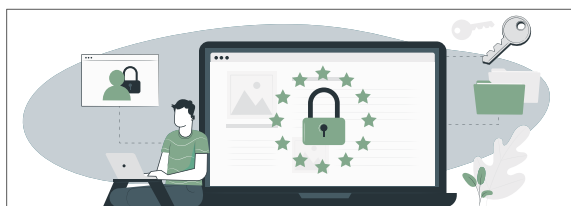
Firewall aplicativoal

A nossa plataforma Speechi Connect está protegida por **um firewall aplicativoal avançado**, garantindo uma camada adicional de segurança. Este firewall aplicativoal oferece inúmeras vantagens.



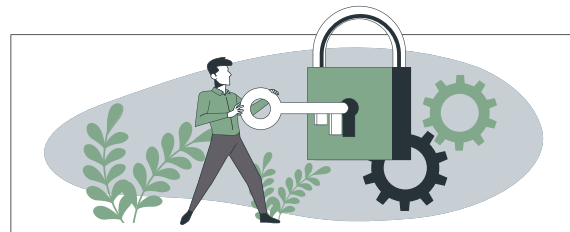
Proteção contra ataques

As tentativas de intrusão são bloqueadas, incluindo ataques por injeção SQL, scripts entre sites (XSS) e outras ameaças comuns.



Monitorização contínua

A análise em tempo real do tráfego de rede permite detectar e prevenir comportamentos suspeitos. O número de requisições por IP em um intervalo de tempo definido é limitado, e os IPs conhecidos por serem maliciosos são colocados em lista negra.

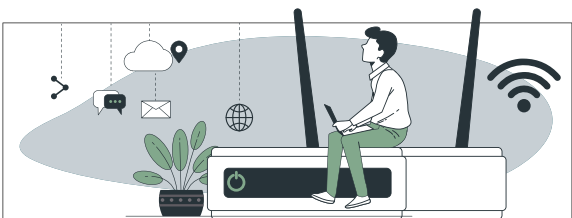


OWASP

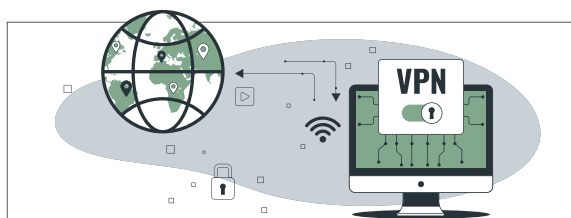
Conforme as regras recomendadas pela OWASP (Open Web Application Security Project), para estar em conformidade com os padrões de segurança internacionais e contribuir para a proteção de dados sensíveis.

Segmentação da infraestrutura

Para garantir uma segurança otimizada da nossa infraestrutura, aplicamos uma segmentação rigorosa.



A utilização de **VLANs** (Redes Locais Virtuais) para isolar diferentes partes da rede e os ambientes, reduzindo assim os riscos de propagação de ameaças.



VPNs (Redes Privadas Virtuais) asseguram conexões seguras e privadas. Os grupos de segurança abrem apenas os fluxos necessários, seguindo o princípio do menor privilégio.



O acesso à infraestrutura é controlado por **sistemas IAM**, garantindo que apenas os utilizadores e serviços autorizados acedam aos recursos necessários, reforçando assim a proteção da nossa infraestrutura e dos nossos dados.



Monitorização e alertas

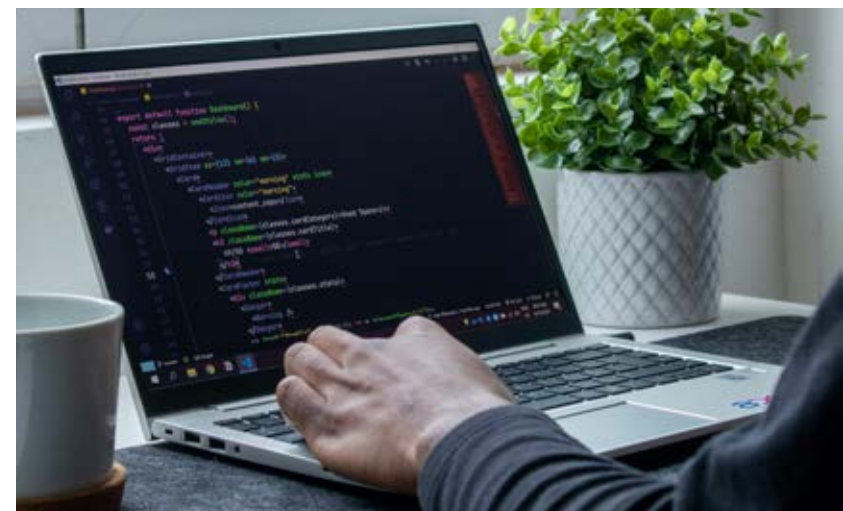
A monitorização e os alertas da plataforma são garantidos 24/7 por um serviço de observabilidade em Cloud, cobrindo tanto os servidores como os dados.

Esta solução permite-nos detectar e reagir rapidamente a anomalias e incidentes, garantindo assim uma disponibilidade e desempenho otimizados.

Auditoria aplicacional

A nossa base de código, assim como as nossas bibliotecas, é regularmente auditada por um serviço de terceiros automatizado. Esta automação permite a deteção de bugs e vulnerabilidades conhecidas, garantindo assim uma segurança otimizada.

Além da auditoria automatizada, realizamos revisões de código manuais e testes de penetração regulares para identificar falhas potenciais antes que se tornem problemáticas. Graças a estas medidas, asseguramos uma proteção contínua e proativa da nossa aplicação.



A nossa plataforma SAAS Speechi Connect foi concebida para oferecer um ambiente de trabalho seguro e em conformidade com as normas mais rigorosas.

Ao combinar tecnologias de ponta e mecanismos de segurança rigorosos, garantimos a proteção dos seus dados e a tranquilidade de espírito de que necessita para se concentrar nas suas atividades profissionais. Para mais informações, não hesite contactar-nos.

