enzo signal

SEGURANÇA E PRIVACIDADE

# Segurança e privacidade incorporadas à arquitetura do Signal.

Esta visão técnica explica exatamente o que a autorização do Microsoft 365 permite, como o Signal trata os dados e quais controles protegem cada etapa da integração.

**O consentimento do administrador habilita o Enzo Signal no ambiente Microsoft da organização. Ele não conecta caixas postais, não transfere e-mails e não concede acesso autônomo ao tenant. Depois da aprovação, cada usuário ainda precisa autenticar e conectar individualmente a própria conta.**

VISÃO TÉCNICA | VERSÃO 1.0 | 6 DE AGOSTO DE 2026

RESUMO EXECUTIVO

# Controles essenciais para uma autorização segura.

| | |
|---|---|
| **Acesso delegado** | O Signal atua em nome do usuário autenticado e dentro das permissões que ele já possui no Microsoft 365. |
| **Sem senha Microsoft** | A autenticação ocorre na Microsoft. A Enzo não recebe nem armazena a senha corporativa do usuário. |
| **Tokens criptografados** | Tokens de acesso e renovação são protegidos no Signal com criptografia autenticada AES-256-GCM. |
| **Infraestrutura privada** | A aplicação roda na AWS em sub-redes privadas, sem IP público, com entrada restrita ao balanceador HTTPS. |
| **IA sem treinamento** | O conteúdo processado pela API da OpenAI não é utilizado para treinar modelos de uso geral por padrão. |
| **Controle reversível** | A organização pode revogar o consentimento e cada usuário pode desconectar sua conta a qualquer momento. |

CONSENTIMENTO NO MICROSOFT 365

# Consentimento administrativo sem acesso autônomo ao tenant.

O Signal utiliza permissões delegadas do Microsoft Graph, e não permissões de aplicação com acesso independente. A autorização administrativa torna o aplicativo elegível para uso na organização; o acesso efetivo só nasce quando cada usuário entra no Signal e conecta sua própria conta.

| | |
|---|---|
| **01** | Revisão e consentimento administrativo<br>O administrador entra na Microsoft, visualiza as permissões solicitadas e concede consentimento para a organização. |
| **02** | Nenhuma caixa é conectada<br>A aprovação, isoladamente, não inicia sincronização, não copia mensagens e não permite que a Enzo escolha usuários ou caixas. |
| **03** | Cada usuário autentica<br>Somente os usuários que entrarem no Signal e conectarem a própria conta geram uma credencial delegada. |
| **04** | O acesso segue o usuário<br>O Signal só pode atuar dentro do alcance que aquele usuário já possui, e a conexão pode ser revogada pela Microsoft ou pelo próprio Signal. |

## O que a aprovação não faz

- Não recebe a senha Microsoft de administradores ou usuários.
- Não utiliza permissões de aplicação para acessar caixas sem um usuário conectado.
- Não conecta automaticamente todos os colaboradores da empresa.
- Não cria uma cópia permanente e integral das caixas postais.
- Não vende dados nem usa conteúdo de e-mail para publicidade.

PERMISSÕES MICROSOFT GRAPH

# Cada permissão existe para uma função visível do produto.

As permissões são delegadas: combinam o escopo aprovado para o Signal com os direitos do usuário autenticado. Elas não ampliam os privilégios que o usuário já possui no Microsoft 365.

| PERMISSÃO | USO NO SIGNAL | CONTROLE |
|---|---|---|
| openid + profile<br>Identidade | Confirmar a identidade Microsoft e associar a conexão à conta correta do Signal. | A autenticação e a senha permanecem sob responsabilidade da Microsoft. |
| offline_access<br>Continuidade da conexão | Renovar o acesso delegado para manter a caixa sincronizada sem exigir novo login a cada atualização. | O token de renovação é criptografado e deixa de ser utilizado após a desconexão ou revogação. |
| Mail.ReadWrite<br>Leitura e organização do Outlook | Ler mensagens e pastas, criar o índice do Signal, refletir estados de leitura, aplicar preferências de organização e trabalhar com rascunhos. | O Signal opera na caixa do usuário conectado e preserva os e-mails originais no Microsoft 365. |
| Mail.Send<br>Envio pelo Outlook | Enviar uma mensagem ou um rascunho quando o usuário confirma essa ação dentro do Signal. | A aprovação administrativa não dispara envios; o envio é uma ação explícita do usuário. |
| Calendars.ReadWrite<br>Calendário do usuário | Ler eventos, relacionar convites recebidos e criar, atualizar ou cancelar eventos solicitados pelo usuário. | As ações são sincronizadas com a agenda Microsoft e permanecem visíveis no Outlook. |
| Calendars.ReadWrite.Shared<br>Calendários compartilhados | Oferecer as mesmas funções em calendários compartilhados aos quais o usuário já tenha acesso. | A permissão não concede ao usuário acesso a calendários que a própria Microsoft não tenha compartilhado com ele. |
| People.Read<br>Contatos e destinatários | Pesquisar pessoas relevantes e contatos frequentes para o preenchimento de destinatários. | É utilizada para sugestões dentro da conta conectada, não para criar um diretório comercial externo. |

ARQUITETURA DE PRODUÇÃO

# Uma superfície pública pequena; serviços e dados protegidos atrás dela.

| | |
|---|---|
| **01** | Borda segura<br>DNS gerenciado, certificado AWS e Application Load Balancer aceitando somente HTTPS com política TLS 1.2/1.3. |
| **02** | Aplicação privada<br>Containers Fargate sem IP público, distribuídos em duas zonas de disponibilidade e acessíveis apenas pelo balanceador. |
| **03** | Dados gerenciados<br>MongoDB Atlas com TLS obrigatório e criptografia AES-256 em repouso; credencial de acesso mantida no AWS Secrets Manager. |
| **04** | Serviços controlados<br>Microsoft Graph e OpenAI acessados por TLS e somente a partir da aplicação; tokens e chaves nunca são expostos ao navegador. |

CONTROLES TÉCNICOS E OPERACIONAIS

# Defesa em camadas, da autenticação ao deploy.

A segurança do Signal não depende de um único controle. Identidade, aplicação, rede, segredos, banco de dados, observabilidade e processo de entrega se complementam.

### Identidade e sessões

- Login por código de uso único, com validade, limite de tentativas e controles de frequência por conta e origem.
- Sessões com tokens de acesso de curta duração, renovação rotativa e capacidade de revogação.
- Estados de autenticação Microsoft assinados, com nonce e expiração para proteger o retorno OAuth.

### Segregação por usuário

- Conexões, índices e preferências são associados ao usuário proprietário em todas as consultas do Signal.
- Atualizações em tempo real exigem sessão autenticada e são entregues em canais exclusivos de cada usuário.
- Origens permitidas são controladas tanto nas APIs web quanto nas conexões em tempo real.

### Rede e infraestrutura

- Aplicação executada em AWS ECS Fargate, em sub-redes privadas e sem endereço IP público.
- A única entrada para a aplicação vem do Application Load Balancer, por HTTPS na porta 443.
- O grupo de segurança dos servidores aceita tráfego somente do balanceador na porta interna da aplicação.

### Criptografia e segredos

- TLS moderno protege o tráfego entre navegador, API, Microsoft Graph e banco de dados.
- Tokens Microsoft recebem uma camada adicional de criptografia autenticada AES-256-GCM antes de serem armazenados.
- Chaves, credenciais e segredos de integração são injetados em runtime pelo AWS Secrets Manager, fora do código e das imagens.

### Monitoramento e continuidade

- Logs centralizados, métricas e alarmes de saúde, disponibilidade, CPU, memória e falhas operacionais no Amazon CloudWatch.
- Verificações independentes de saúde e prontidão impedem que instâncias sem banco disponível recebam tráfego.
- Deploy com circuit breaker e rollback automático se a nova versão não estabilizar.

### Integridade do software

- Imagens de produção imutáveis no Amazon ECR e escaneadas automaticamente quando publicadas.
- Imagem-base do servidor fixada por digest e dependências de produção instaladas de forma reproduzível.
- Segredos, chaves, arquivos locais e exportações de clientes são excluídos do contexto de build.

DADOS E RETENÇÃO

# O Signal mantém o necessário para organizar a experiência, não uma réplica da caixa.

As mensagens e os eventos originais permanecem no Microsoft 365. O Signal mantém um índice operacional e resultados derivados para entregar pesquisa, agrupamento, filtros, resumos e sincronização.

| CATEGORIA | COMO É TRATADA | RETENÇÃO |
|---|---|---|
| **Credenciais Microsoft** | Identificadores da conexão, escopos concedidos e tokens de acesso e renovação criptografados. | Enquanto a integração estiver ativa. Após a desconexão, os tokens são removidos ou inutilizados. |
| **Índice operacional** | Identificadores Microsoft, assunto, prévia, remetentes, destinatários, datas, pasta, estado de leitura e indicadores necessários à navegação. | Enquanto a conta estiver ativa ou enquanto necessário para prestar o serviço. |
| **Resultados do Signal** | Classificações, temas, agrupamentos, resumos, preferências, informações extraídas de convites e demais resultados solicitados. | Enquanto a conta estiver ativa ou até a exclusão aplicável. |
| **Corpo integral e anexos** | São normalmente obtidos do Microsoft Graph quando necessários para exibição ou processamento, sem formar uma cópia permanente e integral da caixa. Trechos, imagens, assinaturas ou conteúdos necessários a uma função podem acompanhar o resultado correspondente. | Conforme a função utilizada e os prazos da conta; o conteúdo original continua sob guarda da Microsoft. |
| **Processamento por IA** | Somente o conteúdo e os metadados necessários à tarefa são enviados à API da OpenAI. Os resultados úteis retornam à conta do usuário. | Entradas e saídas podem ser retidas pelo fornecedor por até 30 dias para operação e prevenção de abuso, salvo configuração contratual menor. |
| **Registros técnicos e de acesso** | Registros mínimos de autenticação, funcionamento, falhas e segurança, sem envio de conteúdo de caixa ao Google Analytics. | Em regra, 14 dias para logs técnicos e 6 meses para registros mínimos exigidos pelo Marco Civil da Internet. |
| **Exclusão da conta** | A solicitação inclui os dados do Signal nos sistemas ativos, ressalvado o mínimo exigido por lei ou para exercício de direitos. | Conclusão em até 15 dias; cópias residuais protegidas deixam de existir nos ciclos regulares de substituição de backups. |

INTELIGÊNCIA ARTIFICIAL

# A IA processa uma tarefa; não passa a ser dona do conteúdo.

O Signal utiliza a API empresarial da OpenAI para classificar mensagens, extrair informações, relacionar conteúdos e gerar resumos ou sugestões. Cada chamada recebe somente o conteúdo e os metadados necessários àquela tarefa.

Os dados enviados pela Enzo à API da OpenAI não são utilizados para treinar modelos de uso geral por padrão. O conteúdo da caixa também não é usado pela Enzo para treinar modelos gerais sem autorização específica.

O processamento é automático. Acesso humano pela equipe Enzo é excepcional, restrito à necessidade de suporte solicitado, investigação de falha ou incidente, proteção da conta, cumprimento legal ou atendimento de direitos.

PRIVACIDADE E GOVERNANÇA

# Papéis claros e uso limitado à prestação do serviço.

- A organização contratante é, em regra, a controladora do conteúdo corporativo; a Enzo atua como operadora conforme as instruções e o contrato aplicável.
- A Enzo é controladora dos dados necessários para administrar contas, segurança, suporte e a relação comercial.
- Os principais operadores são Microsoft, Amazon Web Services, MongoDB, OpenAI e Twilio SendGrid. Google Analytics é limitado às páginas públicas e não recebe conteúdo da caixa postal. Notion somente participa quando o usuário conecta e utiliza essa integração.
- Não vendemos dados pessoais, não compartilhamos conteúdo de e-mail para publicidade comportamental e não transferimos a propriedade do conteúdo do cliente.
- Transferências internacionais são limitadas ao necessário e utilizam mecanismos previstos na LGPD e na regulamentação da ANPD.

## Principais operadores

| | |
|---|---|
| Microsoft | Autenticação, Outlook e execução das ações solicitadas |
| Amazon Web Services | Infraestrutura, rede, registros e gestão de segredos |
| MongoDB | Banco de dados gerenciado |
| OpenAI | Classificação, extração, resumos e sugestões |
| Twilio SendGrid | Comunicações operacionais |
| Google Analytics | Somente páginas públicas; sem conteúdo da caixa postal |
| Notion | Somente quando a integração é conectada e utilizada |

PERGUNTAS FREQUENTES

# Segurança, privacidade e operação da integração.

### 01 O que exatamente acontece quando o administrador aprova o Signal em /mail?

O administrador concede consentimento, dentro da Microsoft, para que o aplicativo possa solicitar as permissões delegadas descritas neste documento. Isso apenas habilita o aplicativo no tenant. Nenhuma caixa é conectada, nenhum e-mail é transferido e nenhum usuário passa a utilizar o Signal automaticamente.

### 02 A aprovação dá à Enzo acesso a todas as caixas da empresa?

Não. O Signal não utiliza permissões de aplicação com acesso autônomo ao tenant. Cada participante precisa entrar no Signal e conectar individualmente sua conta Microsoft. O token resultante representa aquele usuário e está limitado ao que ele próprio pode acessar.

### 03 A Enzo recebe a senha Microsoft do usuário?

Não. Login, senha, MFA e políticas condicionais são tratados diretamente pela Microsoft. O Signal recebe tokens OAuth delegados após a autenticação e os armazena criptografados com AES-256-GCM.

### 04 Por que o Signal precisa de permissão de escrita no e-mail e no calendário?

Porque as funções centrais do produto refletem ações no Outlook: marcar mensagens como lidas ou não lidas, aplicar preferências de organização, trabalhar com rascunhos, enviar quando o usuário confirma e criar ou atualizar eventos escolhidos pelo usuário. Sem essas permissões, o Signal seria uma visualização paralela e não uma caixa sincronizada.

### 05 A autorização administrativa pode enviar e-mails ou alterar agendas sozinha?

Não. A autorização apenas disponibiliza os escopos. Envio de mensagens e ações de calendário ocorrem dentro da conta conectada quando o usuário utiliza e confirma a função correspondente. Preferências configuradas pelo próprio usuário podem automatizar estados de organização, como marcar mensagens selecionadas como lidas.

### 06 Onde ficam os e-mails e eventos originais?

No Microsoft 365. O Signal trabalha sobre a caixa e a agenda existentes por meio da API oficial Microsoft Graph. Não cria uma caixa ou agenda paralela e não mantém uma cópia permanente e integral da caixa postal.

### 07 O que o Signal armazena?

Um índice operacional com metadados necessários à experiência, como assunto, prévia, participantes, datas, pasta e estado; além de preferências e resultados derivados, como classificações, agrupamentos, temas, resumos e informações extraídas. Corpo integral e anexos são normalmente buscados da Microsoft quando necessários. Trechos, imagens, assinaturas ou conteúdo necessário a uma função podem ser mantidos junto ao resultado correspondente.

### 08 Como os dados são criptografados?

O tráfego externo utiliza TLS. A conexão com o MongoDB Atlas também exige TLS, e o Atlas mantém os dados criptografados em repouso com AES-256. Tokens Microsoft recebem ainda uma camada de criptografia autenticada AES-256-GCM dentro da própria aplicação.

### 09 Como a infraestrutura fica isolada da internet?

A API roda em containers AWS Fargate dentro de sub-redes privadas e sem IP público. Somente o Application Load Balancer recebe tráfego externo por HTTPS; os grupos de segurança permitem que o balanceador alcance apenas a porta interna da aplicação. Banco e segredos não são publicados no código ou no frontend.

### 10 Como um usuário é impedido de receber dados de outro?

Conexões, índices e resultados são associados ao identificador do usuário em todas as operações do Signal. As conexões em tempo real também exigem autenticação e usam canais separados por usuário, de modo que atualizações sejam encaminhadas apenas ao proprietário da sessão.

### 11 O conteúdo é usado para treinar inteligência artificial?

Não por padrão. O conteúdo da caixa não é usado pela Enzo para treinar modelos de uso geral sem autorização específica. Os dados enviados pela Enzo à API da OpenAI também não são usados pelo fornecedor para treinar seus modelos por padrão.

### 12 Quanto conteúdo é enviado à OpenAI?

Somente o conteúdo e os metadados necessários para executar a tarefa solicitada, como classificação, extração ou resumo. A OpenAI pode reter entradas e saídas por até 30 dias para operação e prevenção de abuso, salvo configuração contratual menor.

### 13 Pessoas da Enzo conseguem ler os e-mails?

O tratamento é principalmente automático. O acesso humano é excepcional e limitado à necessidade de suporte solicitado, investigação de falha ou incidente, proteção da conta, obrigação legal ou atendimento de direitos, sob dever de confidencialidade e controles de acesso.

### 14 Quais fornecedores participam do tratamento?

Microsoft para autenticação e Outlook; AWS para infraestrutura e segredos; MongoDB para banco de dados; OpenAI para funções de inteligência artificial; e SendGrid para comunicações operacionais. Google Analytics mede apenas páginas públicas e não recebe conteúdo da caixa. Notion participa somente quando essa integração é conectada e utilizada.

### 15 Como a organização interrompe o acesso?

O administrador pode revogar o consentimento do aplicativo no Microsoft Entra, e cada usuário pode desconectar a própria conta no Signal ou revogar a sessão na Microsoft. A desconexão interrompe novos acessos e sincronizações e inutiliza ou remove os tokens mantidos pelo Signal.

### 16 Como funciona a exclusão dos dados?

A organização ou o usuário pode solicitar a exclusão. Os dados da conta são removidos dos sistemas ativos em até 15 dias, ressalvados registros mínimos exigidos por lei ou necessários ao exercício de direitos. Cópias residuais protegidas são eliminadas nos ciclos regulares de substituição de backups.

### 17 O que acontece se houver um incidente de segurança?

A Enzo mantém monitoramento e registros para detectar e investigar eventos. Incidentes capazes de causar risco ou dano relevante são tratados e comunicados à organização, à ANPD e aos titulares afetados nos casos e prazos exigidos pela legislação.

### 18 A integração cria algum acesso irreversível?

Não. A aprovação é revogável, a conexão é individual e o uso pode ser encerrado. Revogar o consentimento impede novos tokens para a organização; desconectar usuários interrompe as sincronizações; e a exclusão dos dados processados pode ser solicitada quando necessário.

DOCUMENTOS E FONTES

# Informações verificáveis.

**Política de Privacidade do Enzo Signal**
https://enzosignal.com/privacy

**Termos de Uso do Enzo Signal**
https://enzosignal.com/terms

**Permissões delegadas do Microsoft Graph**
https://learn.microsoft.com/pt-br/graph/permissions-overview

**Dados enviados à API da OpenAI**
https://developers.openai.com/api/docs/guides/your-data

**Segurança do MongoDB Atlas**
https://www.mongodb.com/docs/atlas/reference/faq/security/

---

CONTATO

# Controle sobre a integração em todas as etapas.

A Enzo disponibiliza suporte para esclarecimentos técnicos, revisão do consentimento Microsoft e orientação sobre revogação e exclusão de dados.

Contato: contact@enzonotes.com

Simplestudio Consultoria e Software Ltda. | CNPJ 19.775.516/0001-36 | Enzo AI - Enzo Signal