WHITE PAPER

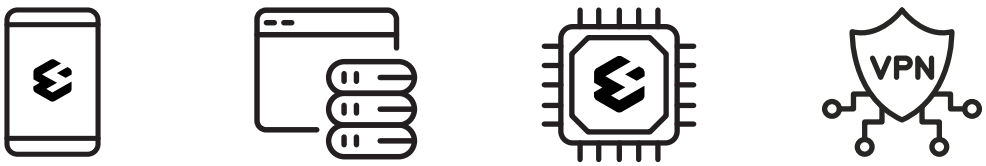
Enigm

Te ofrecemos **seguridad**, **privacidad** y **anonimato** en tus comunicaciones.

Introducción

En este whitepaper, exploraremos en detalle cómo Enigm garantiza la protección de la información del usuario, la confidencialidad de las conversaciones y la anonimidad dentro de la plataforma. Descubrirás cómo Enigm está redefiniendo las normas de la comunicación digital al proporcionar un entorno donde los usuarios pueden conectarse sin temor a la intrusión o la vigilancia no deseada.

Nuestra solución se basa en cuatro componentes esenciales:



App **Servidores** **eSIM** **Red**

App

Funcionalidades

Todas las funcionalidades de Enigm están diseñadas para asegurar que tus comunicaciones sean seguras, privadas y anónimas. Con un enfoque en la innovación y la protección, nuestra app de mensajería te ofrece una herramienta integral para proteger tu privacidad y mantener el control total sobre tus datos.

La app permite enviar mensajes de texto y multimedia, como fotos, videos y documentos, todos ellos protegidos con cifrado de extremo a extremo, garantizando que solo tú y el destinatario puedan acceder a ellos. Además, puedes definir el tiempo de vida de los mensajes, permitiendo que se autodestruyan después de un período específico, eliminando cualquier rastro de la conversación. También puedes adjuntar archivos de manera segura, con la tranquilidad de que están protegidos por el mismo cifrado robusto que asegura tus mensajes. Para proteger tu identidad, los audios enviados pueden ser modulados, de modo que tu voz no sea reconocida. La aplicación incluye un sistema anticapturas de pantalla, que detecta y previene cualquier intento de captura para proteger la confidencialidad de tus mensajes.

En cuanto a las llamadas y videollamadas, puedes realizarlas con la certeza de que están cifradas de extremo a extremo, asegurando que tus comunicaciones sean completamente privadas. Además, durante las llamadas y videollamadas, puedes modular tu voz para proteger tu identidad. Implementamos un sistema que impide la grabación de conversaciones y la captura de videollamadas, garantizando la privacidad total de tus interacciones.

La app también permite la creación de grupos de trabajo, donde las comunicaciones están cifradas y el anonimato de los usuarios es protegido rigurosamente. En estos grupos, los usuarios no pueden ver ni interactuar de manera privada con otros miembros que no tienen como contactos, manteniendo así el anonimato. El creador del grupo tiene la capacidad de definir estrictos controles de permisos, como quién puede enviar mensajes, borrar mensajes, reenviar mensajes, y más, asegurando que el grupo opere bajo un régimen de gobernanza.

FUNCIONES DESTACADAS

Anticapturas de pantalla

Destrucción de mensajes

Modulador de voz

Inhibidor de grabaciones

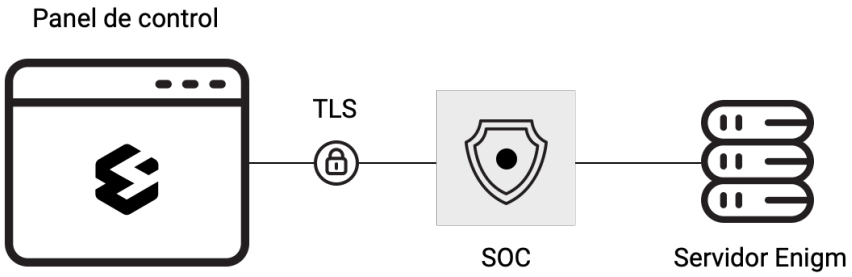
Gestión de permisos

Privacidad de usuarios

> “Enigm **no almacena ningún mensaje en el teléfono**, ni si quiera en cache. Lo que evita la recuperación de datos con técnicas forenses.”

Panel de control

En nuestra plataforma, la seguridad y el control total sobre tu cuenta y dispositivos son aspectos fundamentales. Por ello, hemos desarrollado un panel de control web intuitivo y potente que te permite gestionar todos los aspectos de tu cuenta de forma segura y sencilla. Desde el control de dispositivos conectados hasta la gestión completa de tu cuenta, nuestro panel de control web te proporciona todas las herramientas necesarias para garantizar tu privacidad y seguridad.



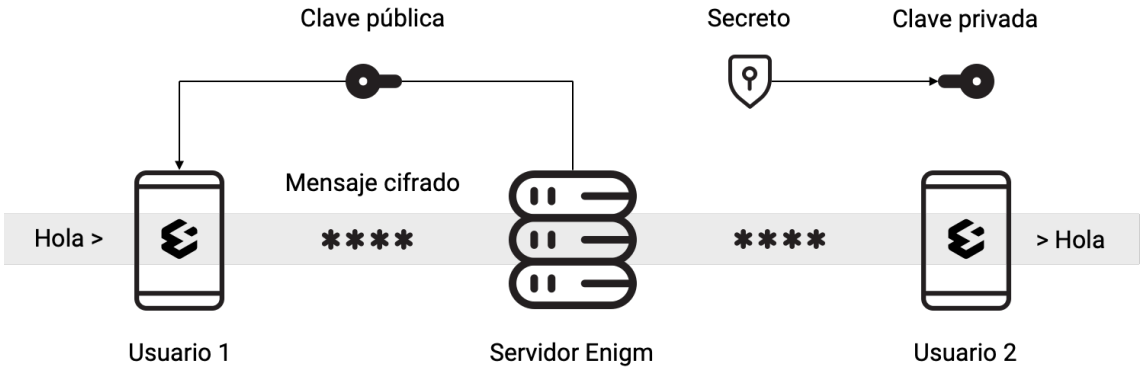
Nuestro panel de control web te permite tener un control exhaustivo sobre los dispositivos conectados a tu cuenta. Puedes ver todos los dispositivos que tienen acceso y, si es necesario, cerrar la sesión de manera remota en cualquiera de ellos, asegurando que solo los dispositivos autorizados tengan acceso a tu cuenta. Además, puedes activar o desactivar las notificaciones push según tus preferencias y necesidades de privacidad, garantizando que solo recibas alertas en los dispositivos que deseas.

La gestión de tu cuenta también es sencilla y segura a través del panel de control web. Puedes decidir si tu cuenta es visible en el servidor público o si prefieres que solo sea accesible en servidores privados, controlando así quién puede encontrarte y comunicarse contigo. Si en algún momento necesitas recuperar tu contraseña, puedes hacerlo utilizando la frase de seguridad generada durante el registro, lo que te permite restablecer tu acceso de manera rápida y segura. También tienes la opción de cambiar tu código PIN y contraseña en cualquier momento para mantener la seguridad de tu cuenta adaptándolos a tus necesidades.

Además, el panel te ofrece la capacidad de eliminar todos los datos asociados a tu cuenta, incluidos mensajes y archivos multimedia, manteniendo solo tu perfil y lista de contactos si así lo deseas. Y si decides que ya no quieres estar en nuestra plataforma, puedes eliminar tu cuenta de manera permanente, desapareciendo por completo y sin dejar rastro alguno, como si nunca hubieras existido.

Cifrado

Integramos la tecnología más avanzada de cifrado y seguridad para proteger la confidencialidad de tus conversaciones. Desde el cifrado AES-256 hasta la utilización de algoritmos post-cuánticos y firmas digitales, nuestro enfoque se centra en garantizar que tus mensajes permanezcan seguros y privados en todo momento.



En nuestro sistema de mensajería, el cifrado es la piedra angular de la seguridad de los datos. Utilizamos el cifrado AES-256 para garantizar que cada mensaje enviado esté protegido de extremo a extremo. AES-256 es un algoritmo de cifrado ampliamente reconocido por su robustez y seguridad, utilizando una clave de 256 bits para proteger los datos de manera efectiva.

Además del cifrado AES-256, implementamos tecnología posts-cuántica para fortalecer aún más nuestra seguridad. Utilizamos el algoritmo Kyber para generar y gestionar las claves de cifrado. Kyber es un esquema criptográfico diseñado específicamente para resistir los ataques de los ordenadores cuánticos, lo que garantiza la longevidad y la seguridad de nuestras claves en un entorno cada vez más avanzado tecnológicamente.

Para asegurar la autenticidad e integridad de los mensajes, cada uno está firmado digitalmente utilizando el algoritmo Dilithium. Esta firma digital proporciona una capa adicional de seguridad al garantizar que los mensajes no hayan sido alterados durante el tránsito y que provienen de la fuente esperada.

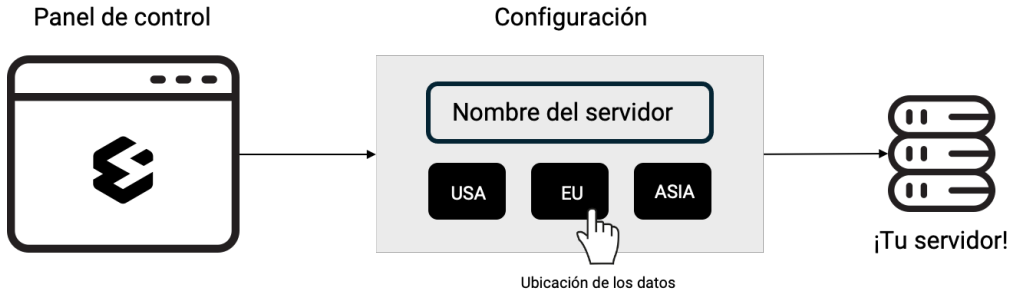
Finalmente, para proteger las claves de cifrado utilizadas en nuestro sistema, implementamos un sistema de secretos que distribuye fragmentos de las claves entre diferentes entidades autorizadas. Este enfoque garantiza que incluso si un fragmento de clave se ve comprometido, no se pueda acceder a la clave completa sin la colaboración de múltiples partes autorizadas.

En resumen, nuestro sistema de mensajería utiliza una combinación de cifrado AES-256, algoritmos post-cuánticos como Kyber, firmas digitales Dilithium y un sistema de secretos para garantizar la seguridad y privacidad de las comunicaciones de nuestros usuarios. Con estas medidas en su lugar, nuestros usuarios pueden comunicarse con confianza, sabiendo que sus datos están protegidos en todo momento.

Servidores

Funcionalidades

Nuestra plataforma también ofrece la flexibilidad y el control que necesitas mediante la posibilidad de configurar y gestionar tus propios servidores. Cualquier usuario de Enigm puede tener sus propios servidores, lo que permite una personalización y control total sobre la infraestructura de sus comunicaciones. Estos servidores pueden ser desplegados en la ubicación geográfica que el usuario prefiera, lo que facilita el cumplimiento de regulaciones locales de datos y optimiza la velocidad y eficiencia de las comunicaciones.



A través de estos servidores, los usuarios pueden indicar a la aplicación que se conecte específicamente a su servidor privado. Esto garantiza que el usuario mantenga un control completo sobre sus datos, asegurando que la información esté siempre bajo su supervisión y gestión. Esta capacidad de dirigir el tráfico de la aplicación hacia un servidor específico proporciona una capa adicional de seguridad y privacidad.

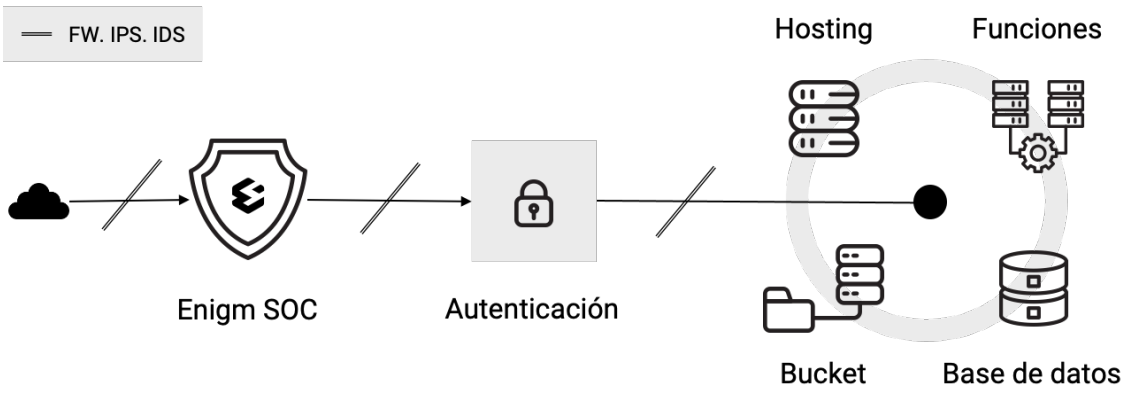
Además, los usuarios tienen la capacidad de eliminar datos de su servidor, incluidos todos los mensajes intercambiados por los miembros que pertenecen a ese servidor. Esta funcionalidad es crucial para mantener la limpieza y seguridad de los datos, permitiendo al usuario gestionar su información de manera eficaz.

La administración de los miembros del servidor es otra característica esencial. Los usuarios pueden administrar quién tiene acceso al servidor, pudiendo expulsar y eliminar miembros no deseados. Además, pueden optar por borrar únicamente la información que un miembro específico haya dejado en el servidor sin necesidad de eliminar al miembro por completo. Esta flexibilidad en la gestión de usuarios y datos asegura que cada servidor pueda ser personalizado según las necesidades específicas de su propietario.

En resumen, puedes desplegar servidores privados de forma sencilla en ubicaciones geográficas específicas, conectar la aplicación a estos servidores y gestionar datos y miembros de manera integral, garantiza una experiencia de usuario segura, privada y personalizable.

Arquitectura

La arquitectura de nuestros servidores está diseñada con un enfoque meticuloso en la seguridad y la eficiencia. Implementamos una serie de tecnologías avanzadas y prácticas de seguridad rigurosas para asegurar que los datos de nuestros usuarios estén protegidos en todo momento.



En nuestra infraestructura, utilizamos un sistema de firewall de aplicaciones y un sistema de detección de intrusiones (IDS) para proteger nuestras aplicaciones contra amenazas y ataques. Este firewall actúa como la primera línea de defensa, filtrando el tráfico malicioso y asegurando que solo el tráfico legítimo pueda acceder a nuestras aplicaciones. Además, el IDS nos permite detectar y responder rápidamente a cualquier actividad sospechosa que pueda comprometer la seguridad de nuestros sistemas.

Nuestro backend está construido sobre una plataforma que ofrece autenticación, bases de datos en tiempo real, almacenamiento y funciones en la nube. La autenticación asegura que solo los usuarios autorizados puedan acceder a nuestros servicios. Las bases de datos en tiempo real nos permiten gestionar y sincronizar datos de manera eficiente, asegurando una experiencia de usuario fluida y reactiva. El almacenamiento en la nube se utiliza para manejar archivos y otros datos de usuario, mientras que las funciones en la nube nos permiten ejecutar lógica de backend de manera segura y escalable.

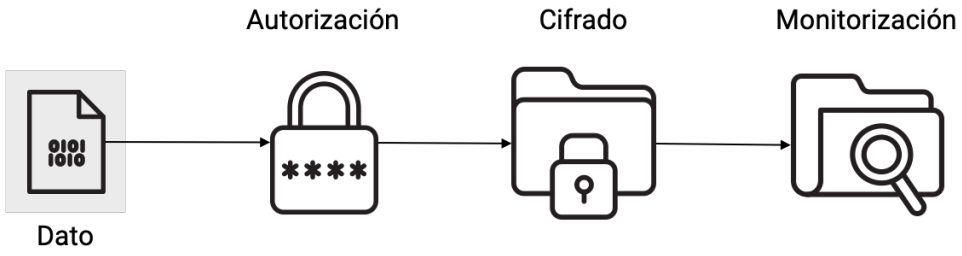
Toda esta infraestructura está protegida bajo un sistema de validación de aplicaciones y configurada con reglas de seguridad estrictas. Estas reglas se aplican tanto a los buckets de almacenamiento como a las bases de datos, garantizando que los datos solo puedan ser accedidos por usuarios y procesos autorizados. Esto asegura que los datos estén protegidos contra accesos no autorizados y que cumplan con los más altos estándares de seguridad.

Además, implementamos sistemas de monitorización de seguridad con IA para supervisar constantemente el estado de nuestra infraestructura y detectar posibles vulnerabilidades. Sin embargo, es importante destacar que estos sistemas de monitorización no almacenan ni analizan ningún dato que pueda identificar a nuestros clientes. Nos enfocamos en mantener la privacidad de nuestros usuarios, asegurando que toda la información personal permanezca confidencial y segura.

En resumen, la arquitectura de nuestros servidores está cuidadosamente diseñada para combinar alta seguridad con eficiencia operativa. Desde la protección perimetral hasta el backend seguro y la monitorización continua, cada componente de nuestra infraestructura trabaja en conjunto para proporcionar un entorno seguro y confiable para nuestras aplicaciones y los datos de nuestros usuarios.

Protección del dato

La protección de los datos en nuestros servidores es una de nuestras máximas prioridades. En un entorno digital donde las amenazas a la seguridad son cada vez más sofisticadas y persistentes, hemos implementado una serie de medidas avanzadas para garantizar que la información de nuestros usuarios permanezca segura y privada en todo momento.



FLUJO DEL DATO

Autorización

Para garantizar la máxima seguridad y privacidad de los datos alojados en nuestros servidores, hemos implementado un riguroso sistema de control de acceso a nivel de registro en nuestra base de datos. Estas reglas, meticulosamente definidas y gestionadas a través de nuestra plataforma backend, desempeñan un papel fundamental en la protección de la información sensible. Cada vez que se realiza una operación de lectura o escritura, estas reglas son evaluadas exhaustivamente, asegurando que solo los usuarios autenticados y debidamente autorizados puedan acceder a los datos correspondientes. Este enfoque no solo proporciona un control preciso sobre quién puede acceder a qué información, sino que también permite una adaptación dinámica a medida que cambian los requisitos de acceso. De este modo, nuestros sistemas garantizan la integridad y la confidencialidad de los datos, asegurando que solo aquellos con los permisos adecuados puedan interactuar con ellos, y fortaleciendo así la seguridad y la privacidad en todas las etapas de la gestión de datos.

Cifrado

Para proteger los datos en nuestros servidores, utilizamos un enfoque avanzado de cifrado. Los datos en reposo están cifrados a nivel de dato con AES-256 y luego tienen un segundo nivel de cifrado aplicado por nuestra plataforma backend, proporcionando una doble capa de seguridad. Además, a nivel de disco, aplicamos un cifrado adicional, asegurando que los datos estén protegidos en todas las capas de almacenamiento. Este triple cifrado asegura que incluso si un nivel de cifrado fuera comprometido, los datos aún permanecerían protegidos.

Para datos que no necesitan ser reversibles, empleamos un proceso de hashing con saltos dinámicos generados aleatoriamente para aumentar la resistencia contra ataques de fuerza bruta. Cada hash se cifra adicionalmente con AES-256, incrementando su seguridad.

Los datos en tránsito están protegidos mediante TLS 1.3, y aplicamos un cifrado transaccional extra para proteger los datos en el payload y prevenir ataques de sniffing. Esto asegura la máxima seguridad en todas las etapas de transmisión y almacenamiento de la información.

Además, implementamos una política de rotación regular de claves a través de nuestro sistema de secretos, lo que incrementa aún más la seguridad. Realizamos auditorías periódicas de nuestros sistemas de cifrado y seguridad para garantizar su efectividad y actualizamos nuestras prácticas para incluir algoritmos resistentes a ataques cuánticos, fortaleciendo así la protección de los datos a largo plazo.

> “Los **datos** almacenados en nuestros servidores solo pueden descifrarse con las claves de tu teléfono y nuestro sistema de secretos. **Enigm no puede descifrarlos.** ”

Monitorización

Para fortalecer aún más la seguridad de Enigm, contamos con un sistema de monitorización respaldado por inteligencia artificial, diseñado para detectar y responder proactivamente a nuevas amenazas. Este sistema garantiza la protección continua de nuestro entorno contra cualquier riesgo potencial. Además, implementamos una retención máxima de logs de 30 días para garantizar la disponibilidad de registros necesarios para análisis posteriores y auditorías de seguridad. Es importante destacar que en nuestros logs no se almacena ningún dato que pueda identificar a nuestros usuarios, y toda la metadata se anonimiza antes de ser registrada por nuestros sistemas de monitorización de seguridad y nuestro equipo de Operaciones de Seguridad (SOC). Esta medida añade una capa adicional de protección de la privacidad de nuestros usuarios, asegurando que sus datos personales estén completamente seguros y protegidos contra cualquier riesgo potencial de exposición.

Privacidad y cumplimiento

Enigm cumple con las regulaciones de privacidad y seguridad de datos aplicables, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Privacidad del Consumidor de California (CCPA). Estamos comprometidos con el cumplimiento de las leyes y regulaciones relevantes para proteger los derechos y la privacidad de nuestros usuarios en todo el mundo.

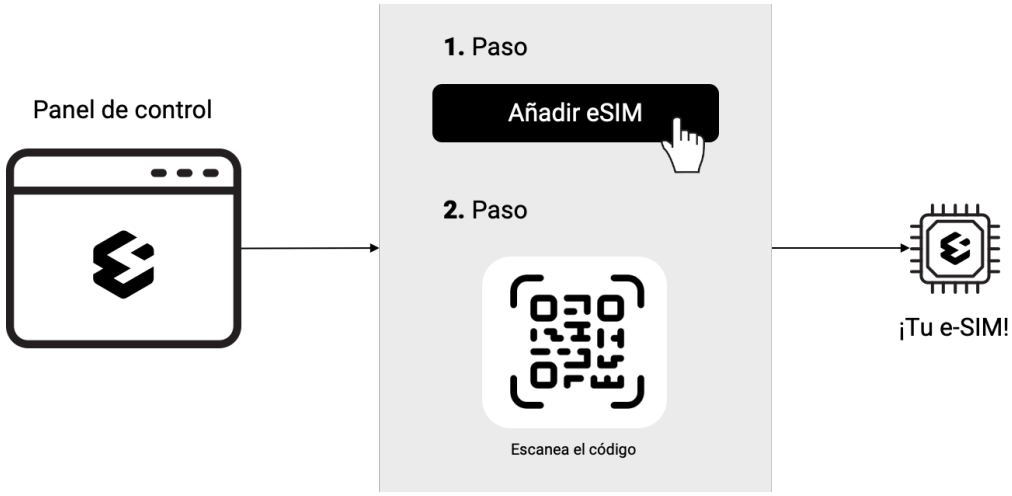
Con Enigm, los usuarios pueden comunicarse con tranquilidad, sabiendo que sus datos están protegidos por una infraestructura de seguridad de vanguardia que prioriza la privacidad y la confidencialidad.

> “No **comprometemos** ni **vendemos** datos de usuarios a terceros.”

eSIM

Funcionalidades

Nuestra eSIM anónima ofrece una serie de funcionalidades únicas que garantizan la seguridad y protección de tus datos en línea.



Al utilizar esta eSIM, tu proveedor de red móvil local no conoce tu número de móvil real, ya que estás en roaming. Esto asegura que no puedan llevarse a cabo ataques como el Ataque SimToolKit, lo que garantiza la integridad y confidencialidad de tus comunicaciones.

Además, nuestra aplicación cuenta con una VPN integrada que añade un valor significativo a la seguridad de tus datos. La VPN cifra todas las comunicaciones de tu dispositivo, garantizando que tu actividad en línea esté protegida contra intrusiones y ataques maliciosos, incluso en redes Wi-Fi públicas o inseguras. Esto proporciona una capa adicional de seguridad al usar nuestra eSIM, asegurando que tus datos estén protegidos en todo momento.

Nuestra eSIM también protege contra la monitorización de la ubicación del suscriptor y el registro de llamadas, mensajes y sesiones de datos, lo que garantiza la privacidad y la confidencialidad de tus actividades en línea. En resumen, nuestra eSIM anónima combinada con la VPN integrada en nuestra aplicación ofrece una solución completa para proteger tus datos y garantizar tu seguridad en línea.

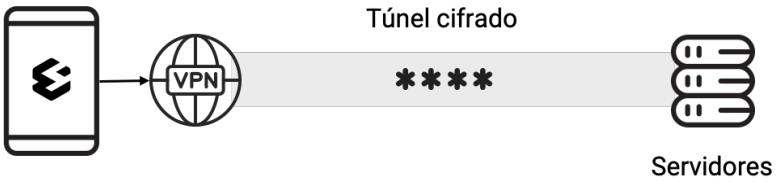
Privacidad y anonimato

Nuestra tecnología eSIM se distingue por ofrecer un servicio exclusivamente enfocado en datos, prescindiendo por completo del número de teléfono. Esta innovadora solución te permite conectar tu dispositivo instantáneamente a la red Global Mobile Data, proporcionándote acceso rápido y confiable a datos móviles en casi cualquier país del mundo, sin requerir verificación de identidad, tarjetas SIM ni documentos. Nuestro servicio se destaca por su total privacidad, ya que no recopilamos ningún dato del usuario.

Red

Funcionalidades

En Enigm, nos comprometemos a brindarte no solo una plataforma de comunicación segura, sino también una capa adicional de protección a través de nuestra VPN integrada y una red de proxys que protegen tu anonimato completo entre tu y nuestros sistemas.



FLUJO CONEXIÓN VPN

Nuestra VPN ofrece una variedad de características que se adaptan a las necesidades de seguridad y privacidad de cada usuario. Una de las funcionalidades clave es la capacidad de elegir si deseas que solo nuestra aplicación utilice el canal seguro de la VPN o si prefieres que todas las aplicaciones instaladas en tu dispositivo se beneficien de esta protección adicional.

Además, nuestra VPN está diseñada para mantenerse activa en todo momento, asegurando que todas tus comunicaciones estén protegidas en todo momento. Incluso si te desconectas del servidor por cualquier motivo, nuestra aplicación se conectará automáticamente a otro servidor de manera inmediata, garantizando una protección constante y sin interrupciones.

Para casos de emergencia, nuestra VPN integrada cuenta con una función de Kill Switch, que actúa como un interruptor de seguridad en situaciones en las que se pierde la conexión a la VPN. Esta función bloquea automáticamente todo el tráfico de tu dispositivo para proteger tu identidad y datos en línea, evitando cualquier exposición no deseada en situaciones de desconexión inesperada.

Privacidad y anonimato

No almacenamos registros ni logs de ninguna índole en nuestros servidores. Esto implica que no tenemos acceso a detalles sobre las conexiones o actividades de navegación de nuestros usuarios. Tu información, incluyendo comunicaciones y actividad en línea, permanece completamente privada mientras utilizas este servicio.

Además, nuestros servidores se encuentran ubicados en territorio offshore para maximizar la privacidad y protección de los datos. Esto significa que están sujetos a leyes y regulaciones que favorecen la confidencialidad de los datos, brindando un entorno seguro y protegido para almacenar la información.

El uso de nuestra VPN añade una capa adicional de cifrado en el transporte de datos, garantizando una mayor seguridad en tus comunicaciones en línea y evitando que tu proveedor de servicios conozca tus destinos de conexión, preservando aún más tu privacidad en línea.

Anexo

Comparación con competidores

En esta comparación, analizaremos las funcionalidades clave y los aspectos de seguridad de nuestra aplicación en comparación con algunos de los principales competidores del mercado. Esto te ayudará a tomar una decisión informada sobre cuál es la mejor opción para tus necesidades de comunicación y seguridad en línea.

No se requiere datos	✓	✗	✓	✗
Antirecuperación de mensajes	✓	✗	✗	✗
Cifrado de extremo a extremo	✓	✓	✓	✓
Criptografía post-cuántica	✓	✓	✗	✗
Servicio de VPN integrado	✓	✗	✗	✗
Modulador de voz	✓	✗	✗	✗
Inhibidor de grabaciones	✓	✗	✗	✗
Anticaptura de pantalla	✓	✓	✗	✗
Servidores privados	✓	✗	✓	✗
Cumplimiento del RGPD	✓	✗	✓	✗