Privacidad y cifrado local: EcoSign no ve tus documentos

La promesa que todos hacen (y pocos cumplen)

"Tu privacidad es importante para nosotros."

Lo habrás leído mil veces.

Pero en la mayoría de las plataformas de firma digital, lo que realmente pasa es esto:

1. Subís tu documento
2. Se sube a sus servidores
3. Lo procesan ahí
4. Te devuelven un resultado

En algún momento, tu documento estuvo en sus manos.

Quizás lo borraron después.

Quizás lo encriptaron.

Quizás ni lo miraron.

Pero estuvo ahí.

EcoSign funciona diferente

En EcoSign, tu documento **nunca sale de tu dispositivo** hasta que vos decides compartirlo.

Y cuando lo compartís con alguien, tampoco pasa por nuestros servidores.

Todo el proceso ocurre en tu ordenador.

¿Cómo es posible eso?

*1. **El documento se procesa localmente***

Cuando subís un PDF a EcoSign:

- Tu navegador lo lee (no nosotros)
- Calcula su "huella digital" (hash SHA-256)
- Lo cifra con una clave que solo vos tenés
- Recién ahí se guarda (cifrado)

En ningún momento nosotros vemos el contenido.

*2. **El cifrado usa claves que no conocemos***

Cuando protegés un documento, se genera una clave de cifrado **en tu dispositivo**.

Esa clave:

- Se deriva de tu sesión (que solo existe en tu navegador)
- Nunca se envía a nuestros servidores
- Se guarda localmente en tu dispositivo
- Se usa para envolver otras claves secundarias

Nosotros no la tenemos. No la podemos recuperar. No la vemos.

*3. **Cuando compartís, el cifrado ocurre antes de enviar***

Si querés compartir un documento con alguien:

1. Generás un enlace seguro

2. El documento **ya está cifrado** antes de salir de tu ordenador

3. La clave para descifrarlo viaja en el enlace (no en nuestros servidores)

4. Quien recibe el enlace descifra localmente

Nosotros solo almacenamos el archivo cifrado. No la clave.

¿Qué significa "cifrado de extremo a extremo"?

Significa que solo las partes involucradas pueden leer el contenido.

En EcoSign:

- **Vos** cifrás el documento en tu ordenador
- **El destinatario** lo descifra en el suyo
- **EcoSign** solo guarda el archivo cifrado y coordina el proceso

Es como enviar una carta en un sobre cerrado. El correo la transporta, pero no puede leer lo que dice.

¿Por qué no simplemente "prometemos no mirar"?

Porque las promesas no son suficientes.

Una plataforma puede prometer privacidad, pero:

- Puede sufrir un hackeo
- Puede recibir una orden judicial
- Puede cambiar de dueño
- Puede cambiar sus políticas
- Puede simplemente mentir

El cifrado de extremo a extremo elimina la necesidad de confianza.

No es que no queramos mirar.

Es que **no podemos** mirar, aunque quisiéramos.

La arquitectura técnica (explicada simple)

Paso 1: Subís un documento

```

Tu ordenador:

1. Lee el PDF

2. Calcula su hash (huella digital)

3. Genera una clave de cifrado

4. Cifra el documento con esa clave

5. Envía el documento cifrado a EcoSign

```

EcoSign recibe: Documento cifrado (ilegible)

EcoSign NO recibe: La clave, ni el contenido

Paso 2: Protegés el documento

```

Tu ordenador:

1. Calcula la evidencia técnica (hash, timestamp)

2. Registra esa evidencia en blockchain (pública)

3. Guarda la clave de cifrado localmente

```

EcoSign recibe: La huella pública (hash)

EcoSign NO recibe: El documento, ni la clave

Paso 3: Compartís con alguien

```

Tu ordenador:

1. Genera un token único

2. Envuelve la clave de cifrado con ese token

3. Crea un enlace con el token incluido

4. Envía el enlace al destinatario

```

```

Ordenador del destinatario:

1. Recibe el enlace

2. Descarga el documento cifrado

3. Usa el token para desenvolver la clave

4. Descifra el documento localmente

```

EcoSign participa: Coordina el enlace y almacena el archivo cifrado

EcoSign NO participa: En el cifrado, descifrado, ni acceso al contenido

¿Y si EcoSign cierra mañana?

Tus documentos siguen siendo verificables.

Porque:

1. **La evidencia está en blockchain** (público, inmutable)

2. **Vos tenés el archivo original**

3. **Vos tenés el ECO (Evidencia Criptográfica de Origen)**

4. **Podés verificar el hash sin necesitar a EcoSign**

El cifrado no es para escondernos de vos. Es para protegerte de nosotros.

La excepción: obligación legal válida

Hay un caso en que un archivo podría ser accedido:

Si una autoridad judicial lo ordena mediante un proceso legal válido.

Pero incluso en ese caso:

- Solo pueden acceder a archivos que **vos** hayás subido cifrados incorrectamente

- No podemos "descifrar" archivos protegidos correctamente

- La evidencia pública (blockchain) no revela el contenido

Nuestra arquitectura hace que sea técnicamente imposible acceder a contenido cifrado de extremo a extremo.

¿Por qué diseñamos EcoSign así?

Porque creemos que:

Tu documento es tuyo. No nuestro. No de nadie más.

Y la mejor forma de garantizar eso no es prometiéndolo.

Es diseñando un sistema donde **no tengamos otra opción**.

Conclusión

En EcoSign:

■ **Tu documento se procesa en tu ordenador**

No en nuestros servidores.

■ **Se cifra con claves que no conocemos**

No podemos acceder al contenido.

■ **Se comparte de forma cifrada**

El destinatario descifra localmente.

■ **Es verificable independientemente**

No necesitás que EcoSign exista para demostrar su validez.

Esto no es marketing. Es arquitectura.

No te pedimos que confíes en nosotros.

Te damos un sistema que no depende de confianza.

Este documento forma parte del material educativo de EcoSign.

Podés protegerlo, firmarlo y verificarlo usando la plataforma.

EcoSign — ecosign.app