DOCUMENTO TÉCNICO

Arquitectura de Seguridad

e.firma Segura

Extensión de Chrome para la Gestión Segura de Credenciales Fiscales

---

Tus e.firmas cifradas con AES-256. El mismo estándar que usan bancos y gobiernos.

Nada sale de tu navegador sin cifrar y sin permiso. Nada.

Versión 1.0 — Marzo 2026
Clasificación: Público

Para el Contador

Este documento explica, en lenguaje claro, cómo funciona la seguridad de nuestra extensión de Chrome. Sabemos que tus e.firmas son la llave de acceso a la vida fiscal de tus clientes. Entendemos la responsabilidad que eso implica. Por eso, antes de pedirte que instales nuestro producto, queremos que entiendas exactamente cómo protegemos esa información.

No necesitas ser experto en tecnología para entender este documento. Hemos incluido analogías y explicaciones sencillas junto con los detalles técnicos para que cualquier contador pueda evaluar si nuestra solución cumple con sus estándares de seguridad.

Compromiso fundamental

Nosotros nunca vemos, accedemos ni almacenamos tus contraseñas y archivos de e.firma en nuestros servidores. Toda la información sensible vive cifrada en tu dispositivo, bajo tu control exclusivo. Si decides usar el respaldo en la nube, los datos se cifran ANTES de salir de tu computadora — ni siquiera nosotros podemos leerlos.

1. Principios de Seguridad

Toda nuestra arquitectura se construye sobre cuatro principios fundamentales. Cada decisión técnica que tomamos se evalúa contra estos principios.

Principio	Qué significa
Conocimiento Cero	Nosotros no podemos ver tus datos. Ni ahora, ni nunca. Ni siquiera si nos lo pidiera un juez, porque técnicamente no tenemos acceso.
Solo Cifrado Local	Tus datos se cifran y descifran únicamente dentro de tu navegador, en tu computadora. Los datos nunca viajan sin protección.
Mínimo Privilegio	La extensión solo solicita los permisos estrictamente necesarios para funcionar. No accedemos a tu historial, otras contraseñas, ni datos de navegación.

Acceso Intencional	Tus e.firmas únicamente pueden ser autocompletadas al dar click en tu bóveda. No existe forma de que el sitio que accedes solicite e.firmas de tu bóveda.
Acceso Oficial	La extensión únicamente tiene la capacidad de autocompletar tus e.firmas en páginas web oficiales alojadas en sat.gob.mx e imss.gob.mx

2. Qué Datos Almacenamos y Dónde

Es importante que sepas exactamente qué información maneja la extensión y dónde se guarda. La tabla siguiente detalla cada tipo de dato.

Dato	Dónde se almacena	Cifrado	Accesible por nosotros
Contraseña de e.firma	Solo en tu dispositivo	Sí — AES-256-CBC	Nunca
Llave privada (.key)	Solo en tu dispositivo	Sí — AES-256-CBC	Nunca
Certificado (.cer)	Solo en tu dispositivo	Sí — AES-256-CBC	Nunca
RFC	Derivado del Certificado	Derivado del Certificado	Nunca
Razón social	Derivado del Certificado	Derivado del Certificado	Nunca
Etiqueta	Solo en tu dispositivo	Sí — AES-256-CBC	Nunca
Respaldo (opcional)	Nube cifrada (opcional)	Sí — AES-256-CBC	Nunca
Correo electrónico	Nuestro servidor (solo si creas cuenta)	Sí — en tránsito y en reposo	Sí — solo para autenticación
Datos de uso anónimos	Nuestro servidor (si aceptas telemetría)	Sí — en tránsito	Sí — pero son anónimos y agregados

Nota importante

Los archivos .key y .cer originales permanecen donde tú los tengas guardados. La extensión crea una copia cifrada dentro de su almacenamiento protegido. Puedes eliminar esta copia en cualquier momento desde tú bóveda (extensión).

3. Arquitectura de Cifrado

3.1 Tu Contraseña Maestra

Al configurar la extensión por primera vez, creas una Contraseña Maestra. Esta es la única contraseña que necesitas recordar. A partir de ella se genera la llave que cifra y descifra todos tus datos. Es crucial entender que esta contraseña maestra nunca se envía a nuestros servidores ni se almacena en ningún lugar fuera de tu propia memoria.

3.2 Derivación de Llaves

Cuando ingresas tu contraseña maestra, la extensión realiza el siguiente proceso — todo dentro de tu navegador, sin enviar nada a internet:

1. Tu contraseña maestra se hashea dos veces con SHA-256 para generar una llave compuesta de 256 bits: SHA-256(SHA-256(contraseña)).
2. Se genera una semilla aleatoria de 256 bits (almacenada en el encabezado del archivo cifrado) y la llave compuesta se procesa mediante AES-KDF con 300,000 rondas. Esto consiste en cifrar repetidamente la llave compuesta con AES usando la semilla como llave, lo que hace computacionalmente costoso intentar adivinar tu contraseña por fuerza bruta.
3. El resultado se combina con la semilla maestra del archivo (otro valor aleatorio de 256 bits) mediante SHA-256, produciendo la Llave de Cifrado final de 256 bits que se usa para cifrar y descifrar tus datos con AES-256-CBC.
4. La integridad de los datos cifrados se verifica mediante HMAC-SHA-256, lo que garantiza que cualquier manipulación del archivo sea detectada.

5. La llave de cifrado se mantiene en la memoria del navegador solo mientras la sesión está activa. Cuando cierras la extensión o se agota el tiempo de inactividad, la llave se elimina de la memoria. Los valores sensibles en memoria se almacenan XOR-cifrados con sales aleatorias y nunca como texto plano.

¿Qué significan estos términos?

AES-256-CBC es el estándar de cifrado que usan bancos, gobiernos y ejércitos en todo el mundo. El "256" significa que la llave tiene 2^{256} combinaciones posibles — un número tan grande que todas las computadoras del planeta trabajando juntas tardarían miles de millones de años en probar todas las combinaciones. AES-KDF con 300,000 rondas significa que incluso si alguien obtuviera tus datos cifrados, cada intento de adivinar tu contraseña requiere ejecutar 300,000 operaciones de cifrado AES — lo cual hace impráctico un ataque automático. HMAC-SHA-256 actúa como un sello de integridad: si alguien modifica incluso un solo bit del archivo cifrado, el sello no coincidirá y la extensión rechazará el archivo.

3.3 Cifrado de tus e.firmas

Cuando agregas una e.firma a la extensión, el proceso es el siguiente:

1. Seleccionas los archivos .key y .cer desde tu computadora e ingresas la contraseña de la e.firma.
2. La extensión lee y valida los archivos localmente (sin enviarlos a ningún servidor).
3. Se genera un Vector de Inicialización (IV) único y aleatorio de 128 bits (16 bytes) para cada operación de guardado.
4. Los archivos y la contraseña se cifran como parte de la base de datos KDBX4 con tu Llave de Cifrado usando AES-256-CBC, autenticada con HMAC-SHA-256.
5. La base de datos cifrada se almacena como un blob binario en el almacenamiento local protegido de la extensión (chrome.storage.local), el cual está aislado por extensión y no es accesible por otras extensiones ni páginas web.
6. Los archivos originales en tu computadora no se modifican ni se eliminan.

3.4 Descifrado y Uso (Firma con Un Clic)

Cuando necesitas firmar en el portal del SAT:

1. Ingresas tu contraseña maestra.
2. La extensión deriva tu Llave de Cifrado en memoria usando el mismo proceso de AES-KDF.
3. Se verifica la integridad del archivo cifrado mediante HMAC-SHA-256 antes de descifrar.
4. Los datos de la e.firma seleccionada se descifran en memoria.
5. La extensión completa automáticamente los campos del portal del SAT con los datos descifrados.
6. Una vez completada la acción, los datos descifrados se eliminan de la memoria.

Dato clave
Los datos descifrados existen en la memoria de tu navegador únicamente durante el instante que toma completar la firma. No se escriben en disco, no se envían por internet, y se olvidan automáticamente al terminar.

4. Respaldo en la Nube (Opcional)

El respaldo en la nube es completamente opcional. La extensión funciona al 100% sin él. Si decides activarlo, te permite recuperar tus datos si cambias de computadora, reinstalas el navegador, o si tu disco duro falla.

4.1 Cómo Funciona el Respaldo

El principio fundamental es: tus datos se cifran ANTES de salir de tu computadora. Lo que llega a nuestros servidores es un bloque de datos ilegible que nosotros no podemos descifrar.

1. Haz iniciado sesión con tu cuenta de Google (oauth)
2. Todos tus datos de e.firmas viven en un paquete cifrado (KDBX4).

3. El paquete cifrado se transmite por HTTPS (TLS 1.3) a nuestro servidor de respaldo.
4. En el servidor, el paquete se almacena tal cual. Nosotros no tenemos la Llave de Respaldo, por lo que no podemos descifrar el contenido.

4.2 Recuperación de Datos

Para recuperar tus datos en un nuevo dispositivo:

1. Instalas la extensión e inicias sesión con tu cuenta de Google (oauth).
2. La extensión descarga el paquete cifrado del servidor.
3. Ingresas tu contraseña maestra.
4. El paquete se descifra localmente en tu nuevo dispositivo.
5. Tus e.firmas están disponibles nuevamente.

¿Qué pasa si olvido mi contraseña maestra?

Si olvidas tu contraseña maestra, no podemos recuperar tus datos. Esto no es una limitación — es una característica de seguridad. Si nosotros pudiéramos restablecer tu contraseña, significaría que tenemos acceso a tus datos, y eso violaría el principio de conocimiento cero. Te recomendamos guardar tu contraseña maestra en un lugar seguro y separado de tu computadora.

4.3 Infraestructura del Servidor

Para quienes quieran conocer los detalles de dónde se almacena el respaldo cifrado:

- **Ubicación:** Servidores en centros de datos con certificación SOC 2 Tipo II e ISO 27001.
- **Redundancia:** Los respaldos cifrados se replican en al menos dos centros de datos geográficamente separados para proteger contra desastres.
- **Cifrado en reposo:** Además de tu cifrado personal, los discos del servidor usan cifrado AES-256 a nivel de hardware.

- **Acceso:** El acceso a los servidores de respaldo requiere autenticación multifactor y está restringido a personal autorizado. Todo acceso queda registrado en bitácora.
- **Retención:** Si eliminas tu cuenta, tu respaldo cifrado se elimina permanentemente de todos los servidores en un plazo máximo de 30 días.

5. Seguridad de la Extensión de Chrome

5.1 Permisos de la Extensión

La extensión sigue el principio de mínimo privilegio: solo solicita los permisos estrictamente necesarios para funcionar.

Permiso	Por qué lo necesitamos	Qué NO hacemos con él
Acceso al sitio del SAT (sat.gob.mx)	Para detectar los campos de e.firma electrónica y completarlos automáticamente.	No leemos ni almacenamos ningún otro dato del portal. No accedemos a tus declaraciones, acuses ni información fiscal.
Acceso al sitio del IMSS (imss.gob.mx)	Para detectar los campos de e.firma electrónica y completarlos automáticamente.	No leemos ni almacenamos ningún otro dato del portal. No accedemos a tu información.
Almacenamiento local (chrome.storage.local)	Para guardar tus datos de e.firma cifrados de forma persistente en tu computadora.	No guardamos tus datos en la nube a menos que se active manualmente.

5.2 Aislamiento y Protección

- **Sandbox del navegador:** La extensión se ejecuta en un entorno aislado (sandbox) dentro de Chrome. No puede acceder a otras extensiones, pestañas o sitios no autorizadas, ni al sistema operativo directamente.
- **Content Security Policy (CSP):** La extensión implementa políticas estrictas que impiden la carga de scripts externos o la inyección de código malicioso.

- **Sin dependencias externas en runtime:** La extensión no carga código de terceros durante su ejecución. Todas las librerías criptográficas están incluidas en el paquete de la extensión y verificadas por hash.
- **Protección contra manipulación:** Las actualizaciones de la extensión pasan por la verificación de firma de la Chrome Web Store. No se puede inyectar una actualización maliciosa sin que Chrome la detecte.

5.3 Bloqueo Automático

Para protegerte en caso de que te alejes de tu computadora o te olvides de cerrar el navegador, la extensión se bloquea automáticamente en estos escenarios:

- Después de 5 minutos de inactividad (o antes dependiendo del navegador).
- Cuando cierras el navegador.
- Cuando bloqueas tu computadora (Windows/Mac).

Cuando la extensión se bloquea, la Llave de Cifrado se elimina de la memoria inmediatamente. Los datos cifrados permanecen seguros en el almacenamiento local.

6. ¿Contra Qué Te Protegemos?

Queremos ser transparentes sobre qué amenazas cubre nuestra extensión y cuáles están fuera de su alcance.

Amenaza	Protección	Nivel
Alguien roba tu computadora o disco duro	Tus datos están cifrados con AES-256. Sin tu contraseña maestra, son ilegibles.	Protegido
Alguien obtiene acceso a tu email	Si activaste el respaldo en la nube únicamente puede ser descargado con tu cuenta de Google.	Protegido

Alguien obtiene acceso a tu cuenta de Google	Tus datos están cifrados con AES-256. Sin tu contraseña maestra, son ilegibles.	Protegido
Malware en tu red	Las e.firmas almacenadas en tu bóveda no pueden ser accesibles desde discos compartidos en la red	Protegido
Malware en tu computadora (keylogger, etc.)	La extensión no puede protegerte contra malware que ya tiene control de tu sistema operativo.	Fuera de alcance
Hackeo a nuestros servidores	Solo almacenamos datos cifrados. Sin tu contraseña maestra, no pueden descifrarse.	Protegido
Un empleado nuestro intenta acceder a tus datos	Arquitectura de conocimiento cero: ni nuestros ingenieros pueden descifrar tus datos.	Protegido
Intercepción de datos en internet (man-in-the-middle)	Todos los datos se cifran localmente antes de transmitirse, y usamos TLS 1.3 para la comunicación.	Protegido
Alguien conoce tu contraseña maestra	Si alguien obtiene tu contraseña maestra y tiene acceso a tu dispositivo, puede descifrar tus datos.	Fuera de alcance
Vulnerabilidad en el navegador Chrome	Dependemos de la seguridad de Chrome. Google actualiza activamente su navegador contra amenazas.	Responsabilidad compartida

Recomendación

Para máxima seguridad, recomendamos: (1) Usa una contraseña maestra fuerte y única de al menos 12 caracteres. (2) Mantén tu navegador Chrome actualizado. (3) Usa un antivirus actualizado. (4) No compartas tu contraseña maestra con nadie. (5) Activa el bloqueo de pantalla en tu computadora.

7. Cumplimiento Normativo

Nuestra extensión está diseñada para cumplir con las regulaciones mexicanas aplicables.

- **Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP):** Cumplimos con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Nuestro aviso de privacidad detalla el tratamiento de datos personales.
- **Regulaciones del SAT sobre e.firma:** La extensión no modifica, altera ni interfiere con el funcionamiento de la e.firma. Simplemente automatiza el proceso manual de seleccionar archivos e ingresar contraseñas en el portal del SAT.
- **Políticas de la Chrome Web Store:** La extensión cumple con todas las políticas de Google para extensiones de Chrome, incluyendo las políticas de privacidad de datos de usuario.
- **Estándares de cifrado:** Utilizamos exclusivamente algoritmos criptográficos reconocidos internacionalmente (AES-256-CBC, PBKDF2, SHA-256) implementados a través de la Web Crypto API nativa del navegador, que está certificada por FIPS 140-2.

8. Auditoría y Transparencia

Creemos que la confianza se gana con hechos, no con promesas. Estos son nuestros compromisos de transparencia:

- **Reporte de vulnerabilidades:** Si un investigador de seguridad encuentra una vulnerabilidad compartimos los medios para realizar un informe privado. Nos comprometemos a verificar y solucionar las vulnerabilidades lo más rápido posible.
- **Código fuente público:** El código fuente de nuestra extensión está disponible para revisión pública, para que cualquier experto pueda verificar que hacemos lo que decimos.
- **Registro de cambios público:** Cada actualización de la extensión incluye un registro detallado de cambios (changelog) para que sepas exactamente qué cambió.

- **Política de notificación de incidentes:** En caso de cualquier incidente de seguridad, nos comprometemos a notificar a todos los usuarios afectados en un plazo máximo de 72 horas, con detalle completo de lo ocurrido y las medidas tomadas.

9. Resumen Técnico

Para referencia rápida, esta tabla resume los estándares y tecnologías que utilizamos:

Componente	Tecnología / Estándar	Notas
Cifrado simétrico	AES-256-CBC	Estándar del gobierno de EE.UU. para información clasificada. FIPS 197
Derivación de llaves	AES-KDF	300,000 iteraciones
Generación de sal	CSPRNG (256 bits)	Generado mediante Web Crypto API
Vector de inicialización	128 bits, único por operación	Generado mediante Web Crypto API
API criptográfica	Web Crypto API (SubtleCrypto)	Generado mediante Web Crypto API
Almacenamiento local	chrome.storage.local	Aislado por extensión, no accesible por otras extensiones ni páginas web
Protección de valores sensibles en memoria	XOR-cifrados con sales aleatorias	Los valores sensibles nunca se almacenan como texto plano en memoria
Transporte	TLS 1.3	La versión más reciente y segura del protocolo

10. Preguntas Frecuentes de Seguridad

¿Pueden ustedes ver mis contraseñas de eFirma?

No. Nunca. Tu contraseña maestra nunca sale de tu dispositivo, y sin ella es imposible descifrar tus datos. Esta es la esencia de la arquitectura de conocimiento cero.

¿Qué pasa si su empresa cierra?

Tus datos locales siguen funcionando independientemente de nuestra empresa. Si usas respaldo en la nube, te daríamos un plazo de al menos 90 días para descargar tus datos antes de cerrar los servidores.

¿Qué pasa si el SAT cambia su portal?

Nuestro equipo monitorea los cambios en el portal del SAT y actualiza la extensión. Tus datos cifrados no se ven afectados por cambios en el portal. Solo la funcionalidad de autocompletado necesitaría actualizarse.

¿Es legal usar esta extensión?

Sí. La extensión no modifica ni altera la e.firma ni el proceso de firma del SAT. Solo automatiza el proceso manual de ingresar archivos y contraseñas, de la misma manera que un administrador de contraseñas autocompleta formularios de inicio de sesión en cualquier sitio web.

¿Puedo usar la extensión sin crear una cuenta?

Sí. La extensión funciona completamente sin cuenta y sin conexión a internet. Solo necesitas crear una cuenta si deseas activar el respaldo cifrado en la nube.

¿Cómo sé que la extensión no fue modificada maliciosamente?

Las extensiones de Chrome están firmadas digitalmente por Google. Cualquier modificación al código requiere pasar por el proceso de revisión de la Chrome Web Store. Además, el código es público y auditable.

Contacto y Verificación

Si tienes preguntas sobre la seguridad de nuestra extensión, o si eres un profesional de seguridad que desea revisar nuestro código, contáctanos:

- **Reporte de vulnerabilidades:** security@openclinic.mx
- **Soporte general:** support@openclinic.mx

Agradecemos que te tomes el tiempo de leer este documento. La seguridad de tus datos y los de tus clientes es nuestra prioridad absoluta. Si algo de lo que describimos aquí no te convence, queremos saberlo. Tu confianza se gana con transparencia, y este documento es nuestro primer paso.