



Coinfish Capital Advisors LLC

coinfishcapital.com · info@coinfishcapital.com

Programa Escrito de Seguridad de la Información (WISP)

Coinfish Capital Advisors LLC

Versión 2026-10 · Vigente desde el 25 de octubre de 2026. Preparado con referencia a la Regla de Salvaguardas de la FTC, 16 CFR Parte 314 (enmendada en 2021 y 2023). Este documento es solo informativo y no constituye asesoría legal.

Empresa	Coinfish Capital Advisors LLC (CCA), 160 Adams Avenue, Unit D PMB 1008, Hauppauge, NY 11788
Responsable del programa / Persona Calificada	Mark O. Brazier, LL.B., EDFP, Presidente y CEO
Alcance	Información de clientes y garantes que CCA recibe para sus servicios de asesoría: el Portal Seguro para Clientes (portal.coinfishcapital.com), el correo (info@coinfishcapital.com), la laptop y el teléfono de trabajo de la Persona Calificada, y los registros en papel
Documentos relacionados	Aviso de Privacidad del Portal, Política de Conservación y Eliminación de Datos, Resumen del Programa de Seguridad de la Información (Ley SHIELD de NY), Plan de Respuesta a Incidentes (todos versión 2026-10-v1)

¿Aplica la Regla?

- CCA es una firma de consultoría. No es prestamista, corredor, contador público (CPA) ni preparador de impuestos.
- Donde la Ley Gramm-Leach-Bliley y la Regla de Salvaguardas de la FTC apliquen a nuestros servicios, este programa está diseñado para alinearse con la Regla de Salvaguardas de la FTC.
- CCA mantiene este programa en todos los casos, porque maneja información financiera sensible de clientes y garantes.

Exención para entidades pequeñas (314.6)

- Las empresas que guardan información de **menos de 5,000 consumidores** están exentas de 314.4(b)(1) (evaluación de riesgos escrita), 314.4(d)(2) (pruebas de penetración y escaneos), 314.4(h) (plan escrito de respuesta a incidentes) y 314.4(i) (informe anual).
- CCA mantiene **los cuatro de todos modos** como buena práctica y revisa el conteo cada año.

(a) Persona Calificada — 314.4(a)

- **Mark O. Brazier, LL.B., EDFP, Presidente y CEO** supervisa, administra y hace cumplir este programa.
- Ningún proveedor externo administra el programa. Si alguna vez se usa uno, la Persona Calificada sigue siendo responsable y lo supervisa.

(b) Evaluación de riesgos — 314.4(b)

Datos que CCA mantiene

Datos	Dónde se guardan	Sensibilidad
Finanzas del negocio (estado de resultados, balance, calendario de deudas)	Portal (R2 cifrado)	Alta
Declaraciones de impuestos del negocio y personales	Portal	Alta
Estados bancarios	Portal	Alta
Estados financieros personales de garantes e información de identidad en documentos	Portal	Muy alta
Datos de contacto, respuestas de admisión, consentimientos	Base de datos del portal (D1)	Media
Memorandos de preparación asistidos por IA	Base de datos del portal, solo la Persona Calificada	Alta
Consultas del sitio web	Correo empresarial	Baja-media (se guardan hasta 2 años)

Los formularios del portal **rechazan números de Seguro Social y de cuentas o tarjetas**. Los documentos cargados aún pueden contenerlos, por eso todo documento se trata como de sensibilidad muy alta.

Amenazas, probabilidad e impacto

Amenaza	Probabilidad	Impacto	Controles principales
Phishing / robo de inicio de sesión de Google	Media	Alto	Verificación en 2 pasos de Google, administración limitada a un correo, sesión de administrador de 1 hora
Pérdida o robo de laptop/teléfono	Baja-media	Alto	Cifrado de disco completo, bloqueo, borrado remoto, sin archivos de clientes guardados localmente
Cliente envía documentos por correo normal	Media	Media	El portal es la vía obligatoria de carga; la página de contacto lo indica
Error en la aplicación web / falla de control de acceso	Baja	Alto	Pruebas automatizadas (unitarias y de integración), carpetas por cliente, controles del lado del servidor
Pérdida de la clave de cifrado	Baja	Alto (archivos ilegibles)	Respaldo fuera de línea bajo control de la Persona Calificada
Exposición de la clave de cifrado	Baja	Muy alto	Claves guardadas por separado de los datos; nunca en código, registros ni correo
Brecha de un proveedor (Cloudflare, Google)	Baja	Alto	Revisión de proveedores; AES-256-GCM a nivel de objeto además del cifrado del proveedor
Uso indebido interno / de personal nuevo	Baja (hoy)	Alto	Solo la Persona Calificada es administradora; capacitación antes de cualquier acceso
Ransomware en la laptop	Baja	Media	Sin archivos de clientes guardados localmente; el portal es el sistema de registro

- Se revisa **cada año** y después de cualquier cambio importante (nuevo sistema, personal, proveedor o incidente).

(c) Salvaguardas — 314.4(c)

1. **Controles de acceso (c)(1)**
2. Cloudflare Access protege todo el portal.

3. **Administrador:** inicio de sesión con Google, limitado a la cuenta de la Persona Calificada, sesión de 1 hora, más una verificación de correo del lado del servidor.
4. **Clientes:** PIN de un solo uso por correo, sesión de 8 horas; cada cliente ve solo su propia carpeta.
5. Sin inicios de sesión compartidos. El acceso se retira el mismo día que alguien se va.
6. **Inventario de datos (c)(2)** — la tabla de la sección (b); se actualiza cada año.
7. **Cifrado (c)(3)**
8. En tránsito: TLS/HTTPS con HSTS.
9. En reposo: cifrado de almacenamiento R2 **más** AES-256-GCM en cada archivo. Si la clave no está disponible, las cargas y descargas se detienen (falla cerrada). Las claves se guardan por separado de los datos, con un respaldo fuera de línea bajo control de la Persona Calificada.
10. Los enlaces de descarga están firmados, vinculados al usuario y vencen en 5 minutos. El depósito de almacenamiento no tiene URL pública.
11. **Desarrollo seguro (c)(4)**
12. Encabezados de seguridad estrictos (CSP solo propio, HSTS, no-referrer, frame-deny), lista de tipos de archivo permitidos con revisión de contenido, límite de 25 MB, límite de 30 solicitudes por minuto.
13. Todo el conjunto de pruebas debe pasar antes de cada publicación.
14. **Autenticación multifactor (c)(5)**
15. El acceso de administrador requiere la Verificación en 2 pasos de Google.
16. Los clientes ingresan con un PIN de un solo uso por correo.
17. **Conservación y eliminación (c)(6)**
18. Los archivos y datos personales se eliminan **90 días después de cerrar un trabajo** mediante un proceso diario (09:00 UTC: 5 AM ET en verano, 4 AM ET en invierno).
19. Los clientes pueden eliminar archivos en cualquier momento o pedir la eliminación total (se completa en 30 días).
20. Las consultas del sitio web se guardan hasta 2 años.
21. Regla: nada se guarda **más de 2 años después de su último uso** salvo que una necesidad legal o comercial lo requiera, o que la eliminación no sea factible. Las retenciones legales se documentan.
22. La eliminación se registra. Los dispositivos se borran antes de reutilizarse o desecharse.
23. **Gestión de cambios (c)(7)**
24. Cada cambio se prueba localmente, se previsualiza, lo aprueba la Persona Calificada y luego se publica. El texto de las políticas lleva número de versión y fecha.
25. Se guarda una copia de respaldo antes de cada cambio.
26. **Monitoreo de actividad (c)(8)**
27. El registro de auditoría anota cada admisión, carga, carga rechazada, vista, eliminación, acción de administrador, acceso denegado y bloqueo por límite de solicitudes. Nunca contiene el contenido de documentos, instrucciones a la IA ni texto de memorandos.
28. La Persona Calificada revisa el registro de auditoría **cada mes**.

(d) Monitoreo y pruebas — 314.4(d)

Para una empresa de una persona, CCA usa pruebas periódicas en lugar de monitoreo continuo: - Pruebas de seguridad **periódicas** del portal, por un evaluador externo calificado o una autoevaluación documentada. - Un escaneo de vulnerabilidades **cada 6 meses** (escaneo web más una auditoría de dependencias del código), y después de cualquier cambio importante. - Revisión mensual del registro de auditoría y el conjunto de pruebas automatizadas en cada publicación.

(e) Capacitación y personal — 314.4(e)

- La Persona Calificada completa capacitación anual de seguridad y privacidad.

- **Incorporación:** toda persona nueva recibe capacitación (phishing, manejo de documentos, el portal, reporte de incidentes) **antes** de cualquier acceso, y reconoce este WISP por escrito.
- El personal recibe solo el acceso que necesita. Hoy solo la Persona Calificada tiene acceso de administrador.
- Se mantiene un registro de capacitación (nombre, fecha, tema).

(f) Proveedores de servicios — 314.4(f)

Proveedor	Qué hace	Supervisión
Cloudflare	Alojamiento, inicio de sesión (Access), almacenamiento cifrado (R2), base de datos (D1), enrutamiento de correo	Revisión anual de informes SOC 2 / ISO y términos de datos
Workers AI (Cloudflare)	Ayuda a organizar documentos y preparar memorandos	Llamada directa; sin AI Gateway , registros desactivados; los términos de Cloudflare indican que el contenido no se usa para entrenar modelos
Google (Workspace/Gmail)	Inicio de sesión de administrador, correo empresarial	Verificación en 2 pasos activa; revisión anual de términos de seguridad

- CCA elige proveedores capaces de proteger los datos, exige salvaguardas en sus contratos o términos de servicio y revisa sus prácticas de seguridad al menos una vez al año.

(g) Mantener el programa al día — 314.4(g)

- Este WISP se actualiza tras resultados de pruebas, nuevos sistemas, personal o proveedores, cualquier incidente o un cambio en el negocio.
- Revisión completa al menos **una vez al año**.

(h) Respuesta a incidentes — 314.4(h)

- Ver el **Plan de Respuesta a Incidentes** (v1): detectar, contener en horas, evaluar, consultar asesoría legal, notificar, corregir y revisar.
- Notificar a los residentes de NY afectados y a las autoridades según lo exige la Ley SHIELD de NY.
- **Notificación a la FTC (314.4(j), vigente desde el 13 de mayo de 2024):** si se obtiene sin autorización información no cifrada de **500 o más consumidores**, se notifica a la FTC mediante su formulario en línea **lo antes posible y a más tardar 30 días** después del descubrimiento.

(i) Informe anual — 314.4(i)

- CCA no tiene junta directiva. La Persona Calificada redacta un **memorando de revisión anual** como único miembro, que cubre el estado del programa, la evaluación de riesgos, resultados de pruebas, incidentes, revisiones de proveedores y cambios recomendados. Se archiva con este WISP.

Preguntas: info@coinfishcapital.com · Políticas relacionadas en coinfishcapital.com.

La familia de empresas Coinfish incluye Coinfish Capital Advisors, Coinfish ATM Solutions, Coinfish Aviation, Coinfish Global Trade y Coinfish Farms. Cada empresa opera de forma independiente.