PLAN ESCRITO DE SEGURIDAD DE LA INFORMACIÓN (WISP)

Cedar Park Tax Service LLC (SAMPLE — fictional firm)

d/b/a Cedar Park Tax (sample)

Preparado según la ley Gramm-Leach-Bliley y la Safeguards Rule de la FTC (16 CFR Parte 314), siguiendo el esquema de la Publicación 5708 del IRS.

Concepto	Detalle
Fecha de vigencia	1 de diciembre de 2026
Versión	1.0 (español)
Persona Calificada / Coordinador de Seguridad de Datos	A. Sample, EA, Owner / Managing Member
Dueño / responsable principal	A. Sample, EA, Owner / Managing Member
Próxima revisión	1 de diciembre de 2027 (al menos una vez por año o ante cualquier cambio importante)
Distribución	Todo el personal. Disponible para clientes que lo pidan, con autorización del DSC.

Importante - lea esto

Este plan se redactó a partir de las respuestas de la propia firma como punto de partida. No es asesoramiento legal, impositivo ni profesional, no está aprobado ni respaldado por el IRS ni por la FTC, y por sí solo no hace que la firma cumpla ninguna ley. La firma es responsable de revisarlo, adaptarlo, implementarlo y mantenerlo, y debe consultar a un abogado o profesional de seguridad calificado cuando corresponda. La versión en inglés generada con las mismas respuestas puede presentarse ante terceros que la soliciten.

El plan en una página

Cedar Park Tax (sample) maneja información de contribuyentes y clientes que los delincuentes buscan activamente. Este plan describe cómo la firma la protege, quién es responsable y qué pasa si algo sale mal. Según las respuestas de la firma, se identificaron 5 tareas de prioridad alta y 7 mejoras adicionales. Cada una figura abajo con una fecha objetivo; el Coordinador de Seguridad de Datos las sigue hasta completarlas.

Menos de 5.000 consumidores

Según 16 CFR 314.6, las firmas que guardan información de menos de 5.000 consumidores están exentas de §314.4(b)(1) (evaluación de riesgos escrita), §314.4(d)(2) (prueba de penetración anual y análisis de vulnerabilidades semestral), §314.4(h) (plan escrito de respuesta a incidentes) y §314.4(i) (informe anual escrito). Este plan igual incluye la evaluación de riesgos y el plan de respuesta porque la Publicación 5708 del IRS los recomienda y mantenerlos cuesta poco.

Plan de acción

Prioridad	Tema	Qué hacer	Norma	Fecha
Alta	MFA en acceso remoto	Exija MFA para todo acceso remoto.	314.4(c)(5)	31/12/2026
Alta	Cifrado de equipos	Active BitLocker/FileVault (o cifrado de volumen en el NAS) en: Desktop workstation; Laptop. Impresoras/escáneres: active el cifrado o borrado automático si lo permiten.	314.4(c)(3)	31/12/2026
Alta	Capacitación en seguridad	Capacite antes de la temporada de impuestos y una vez por año; junte las constancias firmadas (Anexo D).	314.4(e)(1)	31/12/2026
Alta	Phishing y verificación telefónica	Enseñe al personal a verificar todo pedido de datos, pagos o cambios de credenciales llamando a un número conocido.	314.4(e)(1)	31/12/2026
Alta	Protección contra suplantación de email (nota D)	Publique DKIM y DMARC para que nadie pueda enviar correos falsos en nombre de la firma (registros en el Anexo H).	314.4(c) / Pub 4557	31/12/2026
Media	Contactos para incidentes	Complete la hoja de contactos del Anexo C y guarde una copia impresa fuera de la oficina.	314.4(h)	15/12/2026
Media	Wi-Fi de invitados separado	Cree una red separada para clientes y visitas.	314.4(c)(1)	31/12/2026
Media	Backups fuera de la oficina	Agregue un backup automático y cifrado en la nube o fuera de la oficina, y pruebe una restauración cada trimestre.	314.4(c), (d)(1)	31/12/2026
Media	Administrador de contraseñas	Adopte un administrador de contraseñas empresarial con MFA para todo el personal.	314.4(c)(1)	15/01/2027
Media	Registro de actividad	Active y revise cada mes los registros de inicio de sesión (email, software, NAS).	314.4(c)(8)	15/01/2027
Media	Contratos con proveedores	Obtenga cláusulas escritas de protección de datos de cada proveedor del Anexo G y archívelas.	314.4(f)(2)	30/01/2027
Baja	Seguro cibernético	Evalúe una póliza de ciberseguridad; las aseguradoras suelen preguntar por MFA, backups y autenticación de email.	Buena práctica	01/03/2027

I. Objetivo

Nuestro objetivo al desarrollar e implementar este Plan Escrito de Seguridad de la Información (WISP) es establecer medidas administrativas, técnicas y físicas eficaces para proteger la Información de Identificación Personal (PII) que conserva Cedar Park Tax Service LLC (SAMPLE — fictional firm) ("la Firma"). Este WISP busca cumplir las obligaciones de la Firma bajo la ley Gramm-Leach-Bliley y las reglas de Privacidad Financiera y de Salvaguardas (Safeguards Rule) de la Comisión Federal de Comercio (FTC). Describe cómo la Firma accede, recopila, guarda, usa, transmite y protege la PII.

En este WISP, PII significa el nombre (o inicial) y apellido de un contribuyente, cónyuge, dependiente o empleado combinado con cualquiera de estos datos:

A. Número de Seguro Social (SSN), ITIN, fecha de nacimiento o datos laborales;

B. Número de licencia de conducir o identificación estatal;

C. Datos de ingresos, declaraciones de impuestos, planes de retiro, bienes o inversiones;

D. Números de cuentas financieras, tarjetas de crédito o débito, PIN o contraseñas que permitan acceder a cuentas financieras;

E. Direcciones de email, teléfonos no públicos o datos de contacto del domicilio.

No se considera PII la información obtenida legalmente de fuentes públicas o de registros del gobierno abiertos al público.

II. Propósito

A. Asegurar la seguridad y confidencialidad de toda la PII que conserva la Firma.

B. Proteger la PII contra amenazas o riesgos previsibles para su seguridad o integridad.

C. Proteger contra el acceso o uso no autorizado de la PII que pueda causar robo de identidad, fraude de reembolsos u otro daño.

III. Alcance

Este WISP se aplica a todos los dueños, empleados, personal temporal y contratistas de la Firma, a todas sus ubicaciones (Main office (oficina comercial): [Street address redacted], Windermere, FL 34786; Seasonal annex (shared / coworking): [Street address redacted], Winter Garden, FL) y a todos los registros en papel o electrónicos que contengan PII, dondequiera que estén, incluidos servicios en la nube y equipos personales usados para trabajo de la Firma. La Firma ofrece: individual tax returns (1040), business returns (1120, 1120-s, 1065), bookkeeping / payroll, representación ante el irs.

A. Identificar los riesgos internos y externos razonablemente previsibles para los registros con PII.

B. Evaluar la probabilidad y el daño potencial de esas amenazas, según la sensibilidad de la PII.

C. Evaluar si las políticas, procedimientos, sistemas y medidas actuales son suficientes.

D. Diseñar e implementar medidas que reduzcan esos riesgos, de acuerdo con la Safeguards Rule y las recomendaciones del NIST.

E. Monitorear y evaluar regularmente la eficacia de esas medidas.

IV. Responsables designados

La Firma designa a A. Sample, EA (Owner / Managing Member) como Persona Calificada y Coordinador de Seguridad de Datos (DSC) según 16 CFR 314.4(a). El DSC implementa, supervisa y mantiene este WISP y es responsable de:

- Implementar el WISP, incluidos los procedimientos operativos diarios;
- Identificar todos los lugares donde se guarda PII y designarlos como Activos Protegidos de Acceso Restringido;
- Verificar que todo el personal complete la capacitación en seguridad antes de recibir acceso y luego una vez por año;
- Monitorear y probar el cumplimiento de este plan;
- Seleccionar, contratar y evaluar periódicamente a los proveedores con acceso a PII (Anexo G);
- Revisar este WISP al menos una vez por año y ante cualquier cambio importante en el negocio;
- Informar por escrito al dueño, al menos una vez por año, sobre el estado del programa, los riesgos, los incidentes y los cambios recomendados.

La Firma designa a B. Sample como Vocero (Public Information Officer, PIO). Toda comunicación externa después de un incidente (clientes, policía, medios, socios comerciales) la aprueba el PIO junto con el DSC.

Usuarios autorizados y niveles de acceso

Nombre	Función	Tipo	Nivel de acceso
A. Sample, EA	Owner, preparer	Dueño	Total
B. Sample	Office manager	W-2	Total
C. Sample, CPA	Seasonal preparer	Seasonal W-2	Tax software and client files only

Evaluación de riesgos

La Firma evalúa los riesgos por probabilidad (Baja/Media/Alta) y por impacto en la confidencialidad, integridad y disponibilidad de la información de clientes. Los riesgos altos se tratan primero; los medios se reducen dentro del plan de acción; los bajos pueden ser aceptados por escrito por el DSC. La evaluación se repite al menos una vez por año y después de cualquier incidente o cambio importante.

Riesgo	Probabilidad	Impacto	Medidas actuales	Tratamiento
Phishing / robo de credenciales de email o software	Alta	Alta	MFA en email; MFA en software	MFA en todo; capacitación anual; verificación telefónica
Suplantación de la Firma por email (spoofing)	Alta	Media	Nota del chequeo de email: D	Publicar DKIM y aplicar DMARC (Anexo H)
Ransomware / malware	Media	Alta	antimalware; actualizaciones automáticas; Automáticas, solo locales	Actualizaciones, antimalware, backups cifrados fuera de la oficina con restauraciones probadas

Riesgo	Probabilidad	Impacto	Medidas actuales	Tratamiento
Pérdida o robo de laptop/ teléfono	Media	Alta	Ninguna informada	Cifrado de disco en todos los equipos; borrado remoto en teléfonos
Acceso físico no autorizado a papeles	Baja	Alta	guardado bajo llave; trituración	Muebles con llave, escritorio limpio, visitas acompañadas
Mal uso interno o exceso de acceso (incl. temporales)	Baja	Alta	cuentas individuales	Mínimo privilegio; quitar accesos al fin de temporada; revisar registros cada mes
Filtración en un proveedor	Media	Alta	Ninguna informada	Evaluación de proveedores y cláusulas (Anexo G)
Compromiso del acceso remoto	Media	Alta	Ninguna informada	MFA en toda herramienta remota; desactivar accesos remotos sin uso

Información que maneja la Firma: datos de identidad de contribuyentes (SSN/ITIN, fecha de nacimiento, identificaciones), ingresos y documentos impositivos, datos de cuentas bancarias y reembolsos.

Monitoreo y pruebas: el DSC revisa cada mes las alertas de inicio de sesión y los informes del software de seguridad, prueba los backups con una restauración cada trimestre, revisa los accesos de usuarios antes y después de cada temporada de impuestos y organiza una revisión de vulnerabilidades de los sistemas expuestos a internet al menos una vez por año.

V. Mitigación de riesgos dentro de la firma

Política de recopilación y conservación de PII

A. La Firma recopila solo la PII necesaria para fines comerciales legítimos y obligaciones legales.

B. El acceso a la PII se limita al personal cuyas tareas lo requieren (ver Usuarios autorizados).

C. La PII se guarda solo en estos lugares aprobados: Local file server / NAS, Encrypted USB drives; software de impuestos (Drake Tax); portal de clientes (None). Todo lugar nuevo requiere aprobación del DSC.

D. Los registros se conservan 7 años después del último uso, salvo que la ley exija un plazo mayor, y luego se destruyen de forma segura. El DSC documenta el motivo comercial o legal de ese plazo y lo revisa cada año, de acuerdo con 16 CFR 314.4(c)(6), que exige eliminar los datos a más tardar dos años después del último uso salvo que haya una razón comercial o legal para conservarlos (ver Anexo A).

E. El papel se destruye con trituradora de corte cruzado o un servicio certificado; los medios electrónicos se borran de forma segura o se destruyen antes de desecharlos o devolverlos.

Política de responsabilidad del personal

A. Cada persona recibe este WISP al ingresar y firma la constancia (Anexo D) antes de recibir acceso, y otra vez después de la capacitación anual.

B. El personal cumple las Reglas de Conducta (Anexo B) y avisa de inmediato al DSC ante cualquier sospecha de incidente.

C. Los incumplimientos pueden dar lugar a sanciones, incluido el despido y, si corresponde, acciones legales.

D. El acceso se elimina el mismo día en que una persona deja la Firma o termina su contrato temporal; se cambian las credenciales compartidas que conocía.

Política de divulgación de PII

A. La PII no se divulga sin verificar la identidad de quien la recibe y sin autorización del cliente, salvo que la ley lo exija.

B. Los pedidos de cambio de cuenta bancaria, reembolso o datos de contacto, o de envío de registros, se verifican llamando al cliente a un teléfono que ya figura en el archivo, nunca al que viene en el pedido.

C. La PII de empleados se comparte solo con proveedores de nómina, beneficios y seguros obligados por cláusulas escritas de confidencialidad.

Política de eventos reportables

Toda sospecha de incidente de seguridad de datos se maneja según los Procedimientos ante Incidentes del Anexo C. El DSC administra el seguro cibernético, si existe, y coordina los avisos al Enlace del IRS (Stakeholder Liaison), a organismos estatales, a las personas afectadas y a la FTC cuando corresponda.

VI. Mitigación de riesgos externos

Política de protección de la red

A. El firewall está activado en el router de internet y en cada computadora.

B. Los sistemas operativos y programas se actualizan automáticamente; el DSC verifica cada mes que ningún equipo esté desactualizado.

C. Todas las computadoras tienen antimalware licenciado y actualizado con protección en tiempo real.

D. No se usan para la Firma sistemas operativos ni routers sin soporte del fabricante.

E. Las contraseñas de administración de los routers no son las de fábrica y la administración remota del router está desactivada.

Política de control de acceso

A. Se exige autenticación multifactor (MFA) a toda persona que acceda a cualquier sistema con PII, incluidos el email (Microsoft 365), el software de impuestos, IRS e-Services, el portal de clientes, el almacenamiento en la nube y el acceso remoto, como exige 16 CFR 314.4(c)(5). Toda excepción debe ser aprobada por escrito por el DSC con un control equivalente.

B. Cada usuario tiene una cuenta propia. Se prohíben las cuentas y contraseñas compartidas.

C. Las contraseñas siguen la guía NIST SP 800-63B: frases largas (se recomiendan al menos 14 caracteres), sin reutilizar y cambiadas ante sospecha de compromiso. La Firma adoptará un administrador de contraseñas empresarial (ver plan de acción).

D. Los permisos de administrador en las computadoras se limitan al DSC y al proveedor de IT.

Política de intercambio electrónico de PII

A. La PII nunca se envía como adjunto de email sin protección. Los archivos se intercambian por el portal de clientes (None) o email cifrado; las contraseñas se comparten por otro canal.

B. Los medios extraíbles con PII están cifrados (ej. BitLocker To Go) e inventariados.

C. Se mantiene la autenticación de email (SPF, DKIM, DMARC) en el dominio de la Firma para reducir la suplantación de su nombre (ver Anexo H).

Política de Wi-Fi

A. El Wi-Fi de la Firma usa cifrado WPA2 con una clave fuerte que solo conoce el personal autorizado.

B. Clientes y visitas usan una red de invitados separada que no llega a los equipos de la Firma. (A implementar; ver plan de acción.)

C. No se usa Wi-Fi público para trabajo de la Firma salvo a través de la VPN aprobada.

Política de acceso remoto

A. Método de acceso remoto aprobado: Remote desktop tool (e.g., TeamViewer/SplashTop) without MFA. El acceso remoto exige MFA y se limita a usuarios autorizados.

B. Las sesiones remotas no se dejan desatendidas; los equipos se bloquean solos después de 10 minutos de inactividad.

C. Las oficinas en casa cumplen las mismas medidas físicas y técnicas que la oficina principal.

Política de dispositivos conectados

A. El DSC o el proveedor de IT revisa y configura todo equipo nuevo antes de conectarlo a la red de la Firma.

B. La ejecución automática (AutoRun) de USB y discos está desactivada.

C. Fotocopiadoras, escáneres y computadoras se borran o se destruyen sus discos antes de desecharlos, devolverlos o venderlos.

D. Los teléfonos usados para email de la Firma o MFA tienen bloqueo de pantalla, cifrado y actualizaciones automáticas.

Política de capacitación en seguridad

Todo el personal completa una capacitación en seguridad antes de recibir acceso y al menos una vez por año antes de la temporada de impuestos. Cubre phishing y suplantación, verificación telefónica, manejo seguro de PII, uso de contraseñas y MFA, y cómo reportar incidentes. La asistencia se registra en el Anexo D. El DSC se mantiene al día con las alertas del IRS y de la Security Summit (ej. Publicación 4557 del IRS y e-News for Tax Professionals).

Supervisión de proveedores

La Firma elige proveedores capaces de proteger la información de clientes, les exige medidas de protección por contrato y los vuelve a evaluar al menos una vez por año (16 CFR 314.4(f)). Los proveedores figuran en el Anexo G.

VII. Implementación

A partir del 1 de diciembre de 2026, Cedar Park Tax Service LLC (SAMPLE — fictional firm) adopta este Plan Escrito de Seguridad de la Información en cumplimiento de la ley Gramm-Leach-Bliley y de las reglas de Privacidad Financiera y Salvaguardas de la FTC. El plan se revisará al menos una vez por año y después de cualquier cambio importante o evento de seguridad.

Firma: _____ Fecha: _____
A. Sample, EA - Owner / Managing Member

Firma: _____ Fecha: _____
A. Sample, EA - Coordinador de Seguridad de Datos / Persona Calificada

Anexo A: Conservación y destrucción de registros

Tipo de registro	Conservación	Método de destrucción
Declaraciones y papeles de trabajo de clientes	7 años después de presentada (motivo comercial/legal documentado)	Trituración de corte cruzado / borrado seguro
Documentos fuente de clientes (W-2, 1099, identificaciones)	Devolver originales al cliente; copias escaneadas según lo anterior	Triturar las copias en papel después de escanear
Formularios 8879 (firma de e-file)	3 años desde la fecha de vencimiento de la declaración o la fecha de recepción del IRS, la que sea posterior (IRS Pub. 1345)	Borrado seguro / trituración
Nómina y registros de empleados	Según la ley (en general 4 años o más)	Trituración / borrado seguro
Datos de clientes potenciales (sin contratación)	Eliminar dentro de 90 días	Borrado seguro
Computadoras, discos y fotocopiadoras viejas	Hasta su reemplazo	Borrado certificado o destrucción física; guardar el certificado

El DSC revisa estos plazos cada año; confírmelos con su asesor profesional y las normas estatales aplicables.

Anexo B: Reglas de conducta para proteger la PII de clientes

- Bloquee la pantalla cada vez que se aleje; nunca comparta su contraseña ni sus códigos de MFA.
- Nunca envíe PII por email común, mensajes de texto o apps de mensajería; use el portal de clientes.
- Verifique todo pedido de cambio de datos bancarios o direcciones, o de envío de archivos, llamando al cliente al número que figura en el archivo.
- No instale programas ni extensiones, ni conecte dispositivos USB, sin aprobación del DSC.
- No use email ni almacenamiento personal en la nube para datos de la Firma.
- Guarde los papeles con PII bajo llave; tritúrelos, nunca los tire a la basura.
- No hable de información de clientes en lugares públicos ni en redes sociales.
- Avise de inmediato al DSC si pierde un equipo, recibe un email sospechoso o nota actividad rara: la rapidez importa más que la certeza.

Anexo C: Procedimiento ante incidentes y contactos

Ante una sospecha de incidente: (1) no apague los equipos afectados, desconéctelos de la red; (2) avise de inmediato al DSC; (3) el DSC dirige la contención, preserva la evidencia y coordina los pasos de abajo; (4) documente cada acción con fecha y hora.

Quién	Cuándo	Cómo / notas
Coordinador de Seguridad de Datos	De inmediato	A. Sample, EA - tel.: _____
Proveedor de IT	De inmediato	Owner, with an on-call vendor - tel.: _____
Enlace del IRS (Stakeholder Liaison)	Apenas se sospeche robo de datos	irs.gov/stakeholder-liaison (buscar el enlace del estado de la Firma)

Quién	Cuándo	Cómo / notas
Florida Department of Revenue	Según la guía del estado	Federation of Tax Administrators: taxadmin.org (contactos de alerta estatales)
Policía local / FBI IC3	Si hubo un delito	Denuncia policial; ic3.gov
Aseguradora cibernética	Según la póliza (a menudo 24-72 h)	Póliza N.° _____
Personas afectadas y autoridades estatales	Según la ley estatal (resumen abajo)	Fla. Stat. § 501.171
Comisión Federal de Comercio (FTC)	A más tardar 30 días después del descubrimiento si se obtuvo sin autorización información sin cifrar de 500+ consumidores	Formulario en línea de la FTC (16 CFR 314.4(j))
Cuenta EFIN / e-Services	Si las credenciales de e-file pueden estar comprometidas	Contactar al e-help Desk del IRS; revisar la cuenta de e-Services y la cantidad de declaraciones aceptadas

Resumen de la ley estatal de aviso de filtraciones: Florida

Fla. Stat. § 501.171. Avisar a los residentes de Florida afectados por correo postal o email lo antes posible y a más tardar 30 días después de determinar la filtración (puede haber demora por pedido policial o una determinación documentada de que no habrá daño, que se guarda 5 años y se envía al Departamento en 30 días). Si afecta a 500 o más residentes, avisar al Department of Legal Affairs (Fiscal General) dentro de 30 días (15 días más con causa justificada). Si se avisa a más de 1.000 personas a la vez, avisar a las agencias nacionales de informes crediticios. Los proveedores deben avisar a la firma dentro de 10 días. Los registros con datos personales se deben destruir de forma segura. No avisar puede costar hasta US$500.000 por filtración. Desde 2026 los datos personales incluyen biometría y geolocalización (cap. 2026-52).

Fuente: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html (verificado el 18 de noviembre de 2026). Resumen orientativo; confírmelo con un abogado al momento del incidente.

Federal (FTC). Avisar a la FTC con su formulario en línea lo antes posible y a más tardar 30 días después de descubrir un 'evento notificable' (adquisición no autorizada de información de clientes sin cifrar) que afecte a 500 consumidores o más.

Si hay clientes afectados que viven en otros estados, también pueden aplicarse las leyes de esos estados; el DSC revisa las de cada estado afectado durante el incidente.

Después del incidente, el DSC documenta la causa y la solución, y actualiza este WISP y la evaluación de riesgos (16 CFR 314.4(h)(5)-(7)).

Anexo D: Constancia de lectura de empleados y contratistas

Recibí, leí y entiendo el Plan Escrito de Seguridad de la Información de Cedar Park Tax Service LLC (SAMPLE — fictional firm). Me comprometo a cumplir sus políticas y las Reglas de Conducta, a completar la capacitación requerida y a avisar de inmediato cualquier sospecha de incidente. Entiendo que los incumplimientos pueden dar lugar a sanciones, incluido el despido.

Nombre	Función	Fecha de capacitación	Firma	Fecha
A. Sample, EA	Owner, preparer			
B. Sample	Office manager			
C. Sample, CPA	Seasonal preparer			

Anexo E: Inventario de equipos con PII

Equipo	Ubicación	Usuario principal	PII que guarda/procesa	Cifrado
Desktop workstation	Main office	A. Sample	Tax software and client files	No - acción
Laptop	Travel / seasonal annex	C. Sample	Working copies of returns	No - acción

Anexo F: Personal autorizado a acceder a PII

Nombre	Nivel de acceso	Sistemas	Acceso otorgado	Acceso quitado
A. Sample, EA	Total	Software, portal		
B. Sample	Total	Software, portal		
C. Sample, CPA	Tax software and client files only	Software, portal		

Anexo G: Proveedores con acceso a PII

Proveedor	Servicio	¿Cláusulas de protección? (S/N, fecha)	Última revisión
Drake Tax	Software de impuestos		
Microsoft 365	Email		
None	Portal de documentos de clientes		
Owner, with an on-call vendor	Soporte IT (acceso de administrador)		
Example Payroll Co.	Payroll processing (sample)		
Example Bank	Business checking (sample)		

Anexo H: Chequeo de suplantación de email

Dominio: example-sample.invalid Nota: D (56/100) [SIMULADO para esta muestra]

SPF present (~all). DKIM not found on common selectors. No DMARC record. This is a simulated check for the public sample.

Corrección	Tipo	Host	Valor
Publish a DMARC record (start with p=none, then move to reject)	TXT	_dmarc	v=DMARC1; p=none; rua=mailto:dmarc-reports@example-sample.invalid; fo=1
Turn on DKIM signing at your email provider	CNAME/TXT	see provider	generated by your email provider

Chequeo pasivo de registros DNS públicos únicamente. Vuelva a chequear después de los cambios y en cada revisión anual.

Anexo I: Correspondencia con la Safeguards Rule de la FTC

16 CFR 314.4	Requisito (resumen)	Dónde está en este plan
(a)	Persona Calificada	Sección IV
(b)	Evaluación de riesgos escrita (exenta <5.000; incluida)	Evaluación de riesgos
(c)(1)	Controles de acceso	Control de acceso; Usuarios autorizados
(c)(2)	Inventario de datos, equipos y sistemas	Anexos E, F, G
(c)(3)	Cifrado en tránsito y en reposo	Intercambio electrónico; plan de acción
(c)(4)	Desarrollo seguro (apps propias)	No aplica: sin aplicaciones propias
(c)(5)	Autenticación multifactor	Control de acceso
(c)(6)	Destrucción segura; revisión de conservación	Política de conservación; Anexo A
(c)(7)	Gestión de cambios	Dispositivos conectados; Protección de la red
(c)(8)	Monitoreo y registro de actividad	Monitoreo y pruebas; plan de acción
(d)	Pruebas / monitoreo ((d)(2) exenta <5.000)	Evaluación de riesgos: monitoreo y pruebas
(e)	Capacitación y personal calificado	Política de capacitación; Anexo D
(f)	Supervisión de proveedores	Supervisión de proveedores; Anexo G
(g)	Evaluar y ajustar	Sección VII; revisión anual
(h)	Plan de respuesta a incidentes (exento <5.000; incluido)	Anexo C
(i)	Informe anual escrito al dueño/directorio (exento <5.000)	Sección IV (tareas del DSC)
(j)	Aviso a la FTC, 500+ consumidores, dentro de 30 días	Anexo C

Registro de revisiones

Fecha	Revisado por	Cambios

Aviso legal

Este plan se redactó a partir de las respuestas de la propia firma como punto de partida. No es asesoramiento legal, impositivo ni profesional, no está aprobado ni respaldado por el IRS ni por la FTC, y por sí solo no hace que la firma cumpla ninguna ley. La firma es responsable de revisarlo, adaptarlo, implementarlo y mantenerlo, y debe consultar a un abogado o profesional de seguridad calificado cuando corresponda. La versión en inglés generada con las mismas respuestas puede presentarse ante terceros que la soliciten.