Kit WISP en Español

Plan Escrito de Seguridad de la Información para oficinas de impuestos
Plantilla con ejemplo

Neyvis Remón, EA · Zilia Tax Academy
ziliasbc.com

Cómo usar esta plantilla

Con esta plantilla tu oficina tiene su plan escrito de seguridad de datos (WISP) en una tarde. Sigue el mismo orden que la plantilla del IRS (Publicación 5708): objetivo, responsable, riesgos, inventario, medidas de protección, implementación y anexos.

1. Llena cada campo que está **[entre corchetes]** con los datos de tu oficina.
2. Debajo de cada sección hay un **ejemplo ya lleno** de una oficina ficticia. Úsalo como guía, no lo copies tal cual.
3. Borra lo que no aplique a tu oficina y agrega lo que falte. El plan tiene que describir cómo trabajas tú de verdad.
4. Firma la sección 10, guarda una copia impresa y otra digital, y revísalo cada año antes de renovar tu PTIN.

La oficina del ejemplo: Luna Tax Services LLC, en Kissimmee, Florida. La dueña, Rosa Luna, es preparadora con PTIN y tiene una asistente de temporada. Atienden a unos 350 clientes al año, casi todos de habla hispana. Usan un software de impuestos en la nube, correo profesional, una laptop y una computadora de escritorio, y reciben documentos por portal seguro y por WhatsApp.

> **Nota legal:** esta plantilla es material educativo y no es asesoría legal. Está basada en la Regla de Salvaguardas de la FTC (16 CFR Parte 314) y en las Publicaciones 4557 y 5708 del IRS. Cada oficina es responsable de adaptar su plan a sus propios sistemas y riesgos.

1. Objetivo y alcance del plan

- **Nombre de la oficina:** [Nombre legal y nombre comercial]
- **Dirección:** [Dirección de la oficina y de cualquier lugar donde se trabaje, incluida la casa]
- **Número de personas que manejan datos de clientes:** [Número]
- **Clientes atendidos por año (aproximado):** [Número]

Objetivo. Este plan describe cómo [Nombre de la oficina] protege la información personal y financiera de sus clientes, como lo exige la Regla de Salvaguardas de la FTC. Sirve para cumplir tres metas:

- Mantener la información de los clientes confidencial y segura.
- Protegerla contra amenazas y accesos no autorizados que podrían dañar a los clientes.
- Saber qué hacer si ocurre un incidente de seguridad.

Alcance. El plan aplica a toda la información de clientes que la oficina recibe, crea, guarda o envía, en papel o en formato electrónico. Incluye nombres, números de Seguro Social e ITIN, fechas de nacimiento, identificaciones, formularios W-2 y 1099, cuentas bancarias para depósito directo y declaraciones de impuestos. Aplica a la dueña, a los empleados permanentes y de temporada, a los contratistas y a todos los equipos y cuentas que tocan esos datos.

> **Ejemplo: Luna Tax Services LLC**

Luna Tax Services LLC, “Luna Taxes”. Oficina en [dirección], Kissimmee, FL. Rosa Luna también trabaja desde su casa de febrero a abril. Dos personas manejan datos de clientes: Rosa Luna (dueña) y una asistente de temporada. Atienden a unos 350 clientes al año. El plan cubre la oficina, la casa de Rosa, la laptop, la computadora de escritorio, los dos teléfonos de trabajo, el software de impuestos en la nube, el correo profesional, el portal de documentos y el archivo de papel.

2. Persona responsable y usuarios autorizados

La Regla de Salvaguardas pide nombrar a un “Individuo Calificado” que coordine el programa de seguridad. En una oficina de una sola persona, eres tú.

Individuo Calificado: [Nombre, cargo, teléfono, correo]

Sus responsabilidades:

- Implementar y revisar este plan por lo menos una vez al año.
- Dar acceso a los sistemas y quitarlo cuando alguien deja de trabajar en la oficina.
- Capacitar al personal en seguridad.
- Revisar a los proveedores que manejan datos de clientes.
- Dirigir la respuesta si ocurre un incidente.

Usuarios autorizados:

Nombre	Cargo	Sistemas a los que entra	Nivel de acceso	Fecha de alta	Fecha de baja
[Nombre]	[Cargo]	[Sistemas]	[Total / Limitado]	[Fecha]	[Fecha]
[Nombre]	[Cargo]	[Sistemas]	[Total / Limitado]	[Fecha]	[Fecha]

Ejemplo: Luna Tax Services LLC

Individuo Calificado: Rosa Luna, dueña y preparadora con PTIN.

- **Rosa Luna** (dueña, preparadora): software de taxes, correo, portal, nube y archivo físico. Acceso total (administradora) desde el inicio.
- **Asistente de temporada** (recepción y escaneo): portal (solo subir) y software de taxes (solo captura). Acceso limitado, sin acceso a exportar ni a cuentas bancarias. Alta: 15 de enero. Baja: 30 de abril.

3. Inventario de datos, equipos y sistemas

Anota cada lugar donde vive información de clientes. Si no sabes que algo existe, no lo puedes proteger. Incluye los teléfonos y las cuentas personales que uses para el trabajo.

Equipo o sistema	Qué datos guarda	Dónde está	Quién lo usa	Protección actual
[Computadora / laptop]	[Datos]	[Lugar]	[Personas]	[Contraseña, cifrado, antivirus]

Equipo o sistema	Qué datos guarda	Dónde está	Quién lo usa	Protección actual
[Teléfono]	[Datos]	[Lugar]	[Personas]	[Bloqueo, MFA]
[Software de impuestos]	[Datos]	[Nube / local]	[Personas]	[MFA, usuarios]
[Correo]	[Datos]	[Proveedor]	[Personas]	[MFA]
[Portal o nube de documentos]	[Datos]	[Proveedor]	[Personas]	[MFA, cifrado]
[Archivo de papel]	[Datos]	[Lugar]	[Personas]	[Gabinete con llave]
[Impresora o escáner]	[Datos en memoria]	[Lugar]	[Personas]	[Red protegida]
[Red Wi-Fi]	[Tráfico de datos]	[Lugar]	[Personas]	[WPA2/WPA3, red de invitados aparte]

Ejemplo: Luna Tax Services LLC

- **Laptop de Rosa:** declaraciones descargadas y hojas de trabajo; oficina y casa; la usa Rosa. Disco cifrado, contraseña, bloqueo a los 5 minutos y antivirus.
- **Computadora de escritorio:** escaneos temporales; recepción; la usa la asistente. Usuario propio, sin permisos de administrador, antivirus.
- **Teléfono de trabajo de Rosa:** fotos y mensajes de WhatsApp. PIN, borrado remoto y sin copia de fotos a la nube personal.
- **Software de impuestos en la nube:** todas las declaraciones. MFA y un usuario por persona.
- **Correo profesional:** comunicación con clientes. MFA.
- **Portal de documentos:** documentos que suben los clientes. MFA, cifrado y enlaces que vencen.
- **Archivo de papel:** copias firmadas del 8879 y documentos no escaneados. Gabinete con llave y oficina con alarma.
- **Impresora multifunción:** copias en memoria. Conectada solo a la red de la oficina.
- **Wi-Fi de la oficina:** WPA3, clave cambiada cada año y red de invitados aparte para clientes.

4. Evaluación de riesgos

Piensa qué podría salir mal con los datos de tus clientes, qué tan probable es y qué haces para evitarlo. Si tu oficina guarda información de menos de 5,000 personas, la Regla de Salvaguardas no te exige una evaluación de riesgos escrita formal, pero sí revisarla de forma periódica. Esta tabla te sirve para las dos cosas.

Riesgo	Interno o externo	Probabilidad	Impacto	Cómo lo reduzco
[Riesgo]	[Interno / Externo]	[Baja / Media / Alta]	[Bajo / Medio / Alto]	[Medida]
[Riesgo]	[Interno / Externo]	[Baja / Media / Alta]	[Bajo / Medio / Alto]	[Medida]

Fecha de la evaluación: [Fecha] · **Próxima revisión:** [Fecha, antes de renovar el PTIN]

Ejemplo: Luna Tax Services LLC

- **Correo falso (phishing) que roba la contraseña del software.** Externo; probabilidad alta en temporada; impacto alto. MFA en todo, capacitación en enero y nunca entrar por enlaces de correo.

- **Pérdida o robo del teléfono con fotos de WhatsApp.** Externo; media; alto. PIN, borrado remoto y borrar las fotos después de subirlas al portal.
- **Robo de la laptop en el carro o en la casa.** Externo; baja; alto. Disco cifrado y nunca dejarla en el carro.
- **La asistente de temporada se lleva o comparte datos.** Interno; baja; alto. Acceso limitado, acuerdo de confidencialidad firmado y baja de usuarios el 30 de abril.
- **Ransomware en la computadora de escritorio.** Externo; media; alto. Antivirus, actualizaciones automáticas y sin datos guardados localmente.
- **Documentos de papel a la vista de otros clientes.** Interno; media; medio. Escritorio limpio y gabinete con llave.
- **Un cliente manda el Seguro Social por correo o mensaje normal.** Externo; alta; medio. Política de documentos para clientes (Anexo B) y uso del portal.

Fecha: 15 de diciembre de 2026 · Próxima revisión: diciembre de 2027.

5. Medidas de protección

Esta es la parte central del plan: las reglas que la oficina sigue todos los días. Deja las que apliquen, ajusta los detalles entre corchetes y borra las que no correspondan.

5.1 Recolección y conservación de datos

- Solo pedimos la información necesaria para preparar la declaración o dar el servicio contratado.
- Conservamos los registros durante [número] años, por [motivo legal o del negocio]. Pasado ese plazo, los eliminamos de forma segura (sección 5.8).
- Los datos de clientes no se guardan en memorias USB, en cuentas personales ni en el escritorio de la computadora.

5.2 Acceso de usuarios

- Cada persona tiene su propio usuario y contraseña. Nadie comparte cuentas.
- Cada persona tiene solo el acceso que necesita para su trabajo (sección 2).
- Las contraseñas tienen por lo menos [12] caracteres y se guardan en un administrador de contraseñas.
- El acceso se quita el mismo día en que alguien deja de trabajar en la oficina.

5.3 Autenticación de dos pasos (MFA)

- Usamos MFA en todo sistema que contiene datos de clientes: software de impuestos, correo, portal, nube y computadoras cuando el sistema lo permite.
- Si un sistema no ofrece MFA, el Individuo Calificado aprueba por escrito un control igual o más seguro: [describir].

5.4 Cifrado

- Los discos de las computadoras y laptops están cifrados.
- Los datos de clientes se envían solo por canales cifrados: portal seguro o correo cifrado. Nunca enviamos un Seguro Social completo por correo normal ni por mensaje de texto.

- Las copias de seguridad están cifradas.

5.5 Protección de la red y de los equipos

- El Wi-Fi de la oficina usa WPA2 o WPA3, con una clave que no es la de fábrica. Los clientes usan una red de invitados aparte.
- Todos los equipos tienen antivirus y actualizaciones automáticas activadas.
- Las computadoras se bloquean solas después de [5] minutos sin uso.
- Si se trabaja desde casa o fuera de la oficina, nunca se usa Wi-Fi público sin VPN.
- Hacemos copia de seguridad [diaria / semanal] y probamos restaurarla por lo menos [una vez al año].

5.6 Recepción y envío de documentos

- Los clientes suben sus documentos por [nombre del portal].
- Si un cliente manda documentos por WhatsApp o correo, los pasamos al portal o al software el mismo día y los borramos del teléfono o del correo.
- Los teléfonos de trabajo no hacen copia de las fotos en cuentas personales de nube.
- Entregamos a los clientes la política de documentos del Anexo B.

5.7 Oficina física

- Practicamos el escritorio limpio: no dejamos documentos a la vista cuando no los estamos usando ni al final del día.
- Los documentos de papel se guardan en un gabinete con llave.
- Las pantallas no quedan a la vista de los clientes en la sala de espera.

5.8 Eliminación segura

- El papel se tritura con una trituradora de corte cruzado o con un servicio certificado.
- Antes de desechar, vender o donar computadoras, discos o impresoras, se borran de forma segura o se destruyen.
- La información de clientes se elimina a más tardar 2 años después de su último uso, salvo que la ley o una necesidad del negocio exijan conservarla.

5.9 Control de cambios

- Antes de instalar un software nuevo, cambiar de proveedor o conectar un equipo nuevo, el Individuo Calificado revisa cómo afecta la seguridad y actualiza el inventario (sección 3).

> **Ejemplo: Luna Tax Services LLC**
>
> Luna Taxes conserva las declaraciones y los documentos 3 años después de presentarlas. Los formularios 8879 se guardan 3 años, como pide el IRS. Usa un administrador de contraseñas y contraseñas de 14 caracteres. Tiene MFA con aplicación de autenticación en todos los sistemas. Cada domingo hace una copia de seguridad cifrada en la nube y prueba restaurarla en diciembre. Los documentos que llegan por WhatsApp se suben al portal y se borran del teléfono antes de cerrar el día. En la oficina hay trituradora de corte cruzado. La laptop vieja se entrega a un servicio de reciclaje que da certificado de destrucción.

6. Empleados y capacitación

Toda persona que maneja datos de clientes recibe capacitación en seguridad antes de empezar y cada temporada. También firma el acuerdo del Anexo A.

- **Cuándo:** [al contratar y cada año en (mes)]
- **Temas mínimos:** cómo reconocer correos y llamadas falsas, contraseñas y MFA, la política de documentos y WhatsApp, el escritorio limpio y a quién avisar si algo parece raro.
- **Registro:** [nombre, fecha y tema de cada capacitación]
- **Código de conducta:** el personal no instala programas sin permiso, no usa cuentas personales para el trabajo y no comenta datos de clientes fuera de la oficina.
- **Al terminar la relación laboral:** se quitan los accesos el mismo día, se recogen las llaves y los equipos y se cambian las contraseñas compartidas, como la del Wi-Fi.

> **Ejemplo: Luna Tax Services LLC**
>
> La asistente recibe una capacitación de 2 horas el 15 de enero, antes de tocar cualquier dato. Ve ejemplos reales de correos falsos que dicen ser del IRS y practica cómo subir documentos al portal. Firma el Anexo A ese mismo día. Rosa toma un curso de seguridad de datos para preparadores cada año y anota la fecha en el registro.

7. Proveedores de servicios

La oficina solo trabaja con proveedores que pueden proteger los datos de clientes. Se los exige por contrato y los revisa por lo menos una vez al año.

Proveedor	Servicio	¿Maneja datos de clientes?	¿El contrato incluye seguridad?	¿Tiene MFA?	Última revisión
[Nombre]	[Software de impuestos]	[Sí / No]	[Sí / No]	[Sí / No]	[Fecha]
[Nombre]	[Portal o nube]	[Sí / No]	[Sí / No]	[Sí / No]	[Fecha]
[Nombre]	[Soporte de IT]	[Sí / No]	[Sí / No]	[Sí / No]	[Fecha]

> **Ejemplo: Luna Tax Services LLC**
>
> Luna Taxes tiene tres proveedores con acceso a datos: el software de impuestos en la nube, el portal de documentos y un técnico de IT que viene cuando hace falta. Rosa revisa en diciembre los términos de seguridad de los dos servicios en la nube y confirma que el MFA sigue activo. El técnico firmó un acuerdo de confidencialidad y solo entra cuando Rosa está presente.

8. Monitoreo y pruebas

La oficina revisa con regularidad que las protecciones sigan funcionando.

- **Registros de actividad:** revisamos [cada mes] quién entró al software y al portal, y desde dónde.
- **Alertas:** las alertas de inicio de sesión nuevo llegan a [correo del Individuo Calificado].
- **Pruebas:** [cada año] confirmamos que el MFA está activo en todos los sistemas, que las copias de seguridad se pueden restaurar y que las personas que se fueron ya no tienen acceso.
- **Cambios:** si una prueba encuentra un problema o algo cambia en la oficina, actualizamos este plan.

> **Ejemplo: Luna Tax Services LLC**
>
> El primer lunes de cada mes de temporada, Rosa revisa el registro de accesos del software de impuestos. Las alertas de inicio de sesión llegan a su correo y a su teléfono. En diciembre hace la prueba anual: MFA, restauración de la copia de seguridad y lista de usuarios.

9. Plan de respuesta si roban datos

Si ves señales de robo de datos, actúa el mismo día. Las señales más comunes son declaraciones rechazadas porque ya se presentó una con ese Seguro Social, clientes que reciben cartas del IRS que no esperaban, accesos desde lugares raros, correos enviados desde tu cuenta sin que tú los mandaras, o una computadora lenta o que se mueve sola. Si avisas rápido al IRS, puede bloquear declaraciones falsas a nombre de tus clientes.

1. **Contener el daño.** Desconecta de internet el equipo afectado, pero no lo apagues ni lo borres. Cambia las contraseñas desde otro equipo que esté limpio.
2. **Avisar al IRS.** Llama a tu Enlace de Partes Interesadas del IRS (IRS Stakeholder Liaison) de tu estado. El IRS no acepta este tipo de reporte por su línea gratuita general. Ten lista la lista de clientes afectados con nombre y Seguro Social.
3. **Avisar a los estados.** Escribe a la Federación de Administradores Tributarios (StateAlert@taxadmin.org) para saber cómo reportar en cada estado donde preparas declaraciones.
4. **Avisar a las autoridades.** Haz un reporte con la policía local y con la oficina local del FBI.
5. **Avisar a la FTC.** Si el incidente afecta a 500 personas o más, hay que avisar a la FTC en un plazo de 30 días desde que lo descubres.
6. **Avisar a los clientes y al fiscal general del estado.** Cumple la ley de tu estado sobre notificación de filtraciones de datos. Coordina con las autoridades el momento de avisar.
7. **Llamar a tu seguro y a tu soporte de IT.** Si tienes seguro de ciberseguridad, avísale antes de contratar a nadie. Pide ayuda profesional para limpiar los equipos.
8. **Documentar todo.** Anota fechas, horas, qué pasó, a quién avisaste y qué cambiaste. Después, actualiza este plan.

Contactos de emergencia: ver el Anexo C.

> **Ejemplo: Luna Tax Services LLC**

Luna Taxes está en Florida. Según la Ley de Protección de la Información de Florida (Fla. Stat. § 501.171), debe avisar a los clientes afectados a más tardar 30 días después de descubrir la filtración. Si son 500 floridanos o más, también debe avisar al Departamento de Asuntos Legales (la oficina del Fiscal General) en ese mismo plazo. Rosa imprimió los pasos 1 al 8 y los pegó junto a su escritorio. También tiene guardada en el portal una hoja con todos sus clientes, que puede exportar en minutos si el IRS se la pide.

10. Implementación, revisión anual y firma

Cláusula de implementación. [Nombre de la oficina] adopta este Plan Escrito de Seguridad de la Información a partir del [fecha]. El Individuo Calificado es responsable de aplicarlo, de que todo el personal lo conozca y de revisarlo por lo menos una vez al año. También se revisa cuando cambian los sistemas, el personal o los proveedores, y después de cualquier incidente.

Registro de revisiones:

Fecha	Qué se revisó o cambió	Revisó
[Fecha]	[Versión inicial]	[Nombre]
[Fecha]	[Cambios]	[Nombre]

Firma del Individuo Calificado:

Nombre: _____

Firma: _____ Fecha: _____

Dónde se guarda el plan: [copia impresa en (lugar) y copia digital en (lugar seguro)]

Ejemplo: Luna Tax Services LLC

Luna Taxes adopta el plan el 15 de diciembre de 2026. Rosa Luna lo firma como Individuo Calificado. La copia impresa está en el gabinete con llave y la digital, en la nube cifrada de la oficina. Rosa anotó un recordatorio para revisarlo cada diciembre, antes de renovar su PTIN.

Anexo A: Acuerdo de confidencialidad y seguridad para el personal

Yo, [nombre], que trabajo en [Nombre de la oficina] como [cargo], acepto lo siguiente:

1. Uso la información de los clientes solo para hacer mi trabajo y no la comparto con nadie fuera de la oficina.
2. No copio datos de clientes a memorias USB, cuentas personales, mi teléfono personal ni mi correo personal.
3. Mantengo mi contraseña en secreto, uso la autenticación de dos pasos y no dejo mi sesión abierta sin supervisión.
4. Sigo la política de escritorio limpio y guardo los documentos bajo llave.

5. Aviso de inmediato al Individuo Calificado si veo algo sospechoso: un correo raro, un acceso extraño o un documento perdido.
6. Cuando termine mi trabajo, devuelvo llaves, equipos y documentos, y sigo guardando la confidencialidad.

Leí el Plan Escrito de Seguridad de la Información de la oficina y recibí capacitación el [fecha].

Firma: _____ Fecha: _____

Nota: entrega este acuerdo en el idioma que el empleado entienda mejor. La versión en inglés está justo abajo.

Annex A (English): Staff Confidentiality and Security Agreement

I, [name], working at [Office name] as [position], agree to the following:

1. I use client information only to do my job, and I do not share it with anyone outside the office.
2. I do not copy client data to USB drives, personal accounts, my personal phone or my personal email.
3. I keep my password secret, use multi-factor authentication and do not leave my session open unattended.
4. I follow the clean desk policy and keep documents locked away.
5. I immediately notify the Qualified Individual if I see anything suspicious: an unusual email, a strange login or a missing document.
6. When my work ends, I return keys, equipment and documents, and I continue to keep all client information confidential.

I have read the office's Written Information Security Plan and received training on [date].

Signature: _____ Date: _____

Anexo B: Política de documentos para clientes

Entrégala impresa o envíala por mensaje al inicio de la temporada.

Cómo protegemos su información en [Nombre de la oficina]

Su información personal es valiosa, y los ladrones de identidad la buscan sobre todo durante la temporada de impuestos. Por eso le pedimos:

- **Suba sus documentos por nuestro portal seguro:** [enlace]. Es la forma más segura.
- **No nos mande su Seguro Social, su ITIN ni su número de cuenta bancaria por correo normal ni por mensaje de texto.**
- Si nos manda fotos por WhatsApp, las pasamos a nuestro sistema protegido y las borramos de nuestro teléfono el mismo día.
- **Nunca le vamos a pedir contraseñas ni pagos por mensaje de texto.** Si recibe un mensaje así a nuestro nombre, llámenos al [teléfono] antes de responder.
- Guardamos sus documentos durante [número] años y después los destruimos de forma segura.

¿Preguntas? Llámenos al [teléfono].

Anexo C: Contactos de emergencia

Contacto	Para qué	Teléfono o correo
Individuo Calificado	Dirigir la respuesta	[ ]
IRS Stakeholder Liaison de mi estado	Reportar el robo de datos de clientes (búscalo en IRS.gov como “Stakeholder Liaison Local Contacts”)	[ ]
Federación de Administradores Tributarios	Saber cómo reportar a los estados	StateAlert@taxadmin.org
Policía local	Hacer el reporte	[ ]
FBI, oficina local	Hacer el reporte	[ ]
Soporte de IT	Contener y limpiar los equipos	[ ]
Seguro de ciberseguridad	Abrir el reclamo	[ ]
Proveedor del software de impuestos	Bloquear cuentas y revisar accesos	[ ]
Fiscal general del estado	Notificación de filtración, si aplica	[ ]

Fuentes

- IRS, Publicación 5708: *Creating a Written Information Security Plan for your Tax & Accounting Practice*.
- IRS, Publicación 4557: *Safeguarding Taxpayer Data*.
- FTC, Regla de Salvaguardas (16 CFR Parte 314).
- IRS: pasos para profesionales de impuestos con robo de datos (*Data Theft Information for Tax Professionals*).
- Florida, Estatuto 501.171 (Ley de Protección de la Información de Florida).

© 2026 Zilia Tax Academy · Material educativo; no es asesoría legal. Licencia para uso en una oficina.