EJEMPLO LLENO

Plan Escrito de Seguridad de la Información (WISP)

Luna Tax Services LLC
Kissimmee, Florida
Adoptado el 15 de diciembre de 2026

Oficina ficticia. Este ejemplo acompaña al Kit WISP en Español y muestra cómo se ve un plan terminado. No lo copies tal cual: tu plan tiene que describir tu oficina.

Neyvis Remón, EA · Zilia Tax Academy · ziliasbc.com

Datos de la oficina

- **Nombre de la oficina:** Luna Tax Services LLC (“Luna Taxes”)
- **Dirección:** [dirección], Kissimmee, FL. Rosa Luna también trabaja desde su casa de febrero a abril.
- **Personas que manejan datos de clientes:** 2 (Rosa Luna, dueña, y una asistente de temporada)
- **Clientes atendidos por año:** unos 350

1. Objetivo y alcance del plan

Objetivo. Este plan describe cómo Luna Tax Services LLC 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: 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.

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. Aplica a la dueña, a la asistente de temporada y a cualquier contratista.

2. Persona responsable y usuarios autorizados

Individuo Calificado: Rosa Luna, dueña y preparadora con PTIN. [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	Nivel de acceso	Alta	Baja
Rosa Luna	Dueña, preparadora	Software de taxes, correo, portal, nube, archivo físico	Total (administradora)	Desde el inicio	—
Asistente de temporada	Recepción y escaneo	Portal (solo subir), software de taxes (solo captura)	Limitado, sin exportar ni ver cuentas bancarias	15 de enero	30 de abril

3. Inventario de datos, equipos y sistemas

Equipo o sistema	Qué datos guarda	Dónde está	Quién lo usa	Protección
Laptop de Rosa	Declaraciones descargadas, hojas de trabajo	Oficina y casa	Rosa	Disco cifrado, contraseña, bloqueo a los 5 minutos, antivirus
Computadora de escritorio	Escaneos temporales	Recepción	Asistente	Usuario propio sin permisos de administrador, antivirus
Teléfono de trabajo de Rosa	Fotos y mensajes de WhatsApp	Con Rosa	Rosa	PIN, borrado remoto, sin copia de fotos a la nube personal
Software de impuestos en la nube	Todas las declaraciones	Proveedor en la nube	Rosa y asistente	MFA, un usuario por persona
Correo profesional	Comunicación con clientes	Proveedor en la nube	Rosa	MFA
Portal de documentos	Documentos que suben los clientes	Proveedor en la nube	Rosa y asistente	MFA, cifrado, enlaces que vencen
Archivo de papel	Copias firmadas del 8879 y documentos no escaneados	Gabinete en la oficina	Rosa	Gabinete con llave, oficina con alarma
Impresora multifunción	Copias en memoria	Oficina	Ambas	Conectada solo a la red de la oficina
Wi-Fi de la oficina	Todo el tráfico	Oficina	Ambas	WPA3, clave cambiada cada año, red de invitados aparte

4. Evaluación de riesgos

Riesgo	Tipo	Probabilidad	Impacto	Cómo lo reducimos
Correo falso (phishing) que roba la contraseña del software	Externo	Alta en temporada	Alto	MFA en todo, capacitación en enero, nunca entrar por enlaces de correo
Pérdida o robo del teléfono con fotos de WhatsApp	Externo	Media	Alto	PIN, borrado remoto, borrar las fotos después de subirlas al portal
Robo de la laptop en el carro o en la casa	Externo	Baja	Alto	Disco cifrado, nunca dejarla en el carro
La asistente de temporada se lleva o comparte datos	Interno	Baja	Alto	Acceso limitado, acuerdo de confidencialidad, baja de usuarios el 30 de abril
Ransomware en la computadora de escritorio	Externo	Media	Alto	Antivirus, actualizaciones automáticas, 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 de la evaluación: 15 de diciembre de 2026 · **Próxima revisión:** diciembre de 2027

5. Medidas de protección

5.1 Recolección y conservación de datos

- Solo pedimos la información necesaria para preparar la declaración o dar el servicio contratado.
- Conservamos las declaraciones y los documentos 3 años después de presentarlas. Los formularios 8879 se guardan 3 años, como pide el IRS. 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 14 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 con aplicación de autenticación en todos los sistemas con datos de clientes: software de impuestos, correo, portal y nube.

5.4 Cifrado

- Los discos de la laptop y de la computadora de escritorio están cifrados.
- Los datos de clientes se envían solo por el portal seguro o por 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 WPA3, con una clave que se cambia cada año. 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.
- Cuando Rosa trabaja desde casa o fuera de la oficina, nunca usa Wi-Fi público sin VPN.
- Cada domingo se hace una copia de seguridad cifrada en la nube, y en diciembre se prueba restaurarla.

5.6 Recepción y envío de documentos

- Los clientes suben sus documentos por el portal seguro de la oficina.
- Los documentos que llegan por WhatsApp o correo se suben al portal y se borran del teléfono o del correo antes de cerrar el día.
- 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, en una oficina con alarma.
- Las pantallas no quedan a la vista de los clientes en la sala de espera.

5.8 Eliminación segura

- El papel se tritura con la trituradora de corte cruzado de la oficina.
- Los equipos viejos se entregan a un servicio de reciclaje que da certificado de destrucción.
- 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, Rosa revisa cómo afecta la seguridad y actualiza el inventario (sección 3).

6. Empleados y capacitación

- **Cuándo:** al contratar y cada año en enero, antes de la temporada.
- **Capacitación de la asistente:** 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.
- **Capacitación de Rosa:** un curso de seguridad de datos para preparadores cada año.
- **Registro:** nombre, fecha y tema de cada capacitación, guardado junto a este plan.
- **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 (a más tardar el 30 de abril para la asistente de temporada), se recogen las llaves y los equipos y se cambian las contraseñas compartidas, como la del Wi-Fi.

7. Proveedores de servicios

Proveedor	Servicio	¿Maneja datos?	¿Contrato con seguridad?	¿MFA?	Última revisión
[Nombre]	Software de impuestos en la nube	Sí	Sí	Sí	Diciembre 2026
[Nombre]	Portal de documentos	Sí	Sí	Sí	Diciembre 2026
[Nombre]	Técnico de IT (cuando hace falta)	Sí	Acuerdo de confidencialidad firmado	No aplica	Diciembre 2026

Rosa revisa cada diciembre los términos de seguridad de los dos servicios en la nube y confirma que el MFA sigue activo. El técnico de IT solo entra cuando Rosa está presente.

8. Monitoreo y pruebas

- **Registros de actividad:** el primer lunes de cada mes de temporada, Rosa revisa quién entró al software de impuestos y al portal, y desde dónde.
- **Alertas:** las alertas de inicio de sesión nuevo llegan al correo y al teléfono de Rosa.
- **Prueba anual (diciembre):** MFA activo en todos los sistemas, restauración de la copia de seguridad y lista de usuarios (nadie que se fue sigue con acceso).
- **Cambios:** si una prueba encuentra un problema o algo cambia en la oficina, se actualiza este plan.

9. Plan de respuesta si roban datos

Señales de alerta: 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 nuestra cuenta sin que los mandáramos, o una computadora lenta o que se mueve sola. Ante cualquiera de ellas, actuamos el mismo día:

1. **Contener el daño.** Desconectar de internet el equipo afectado, sin apagarlo ni borrarlo. Cambiar las contraseñas desde otro equipo limpio.
2. **Avisar al IRS.** Llamar al IRS Stakeholder Liaison de Florida, con la lista de clientes afectados (nombre y Seguro Social) a mano. La hoja de clientes está guardada en el portal y se exporta en minutos.
3. **Avisar a los estados.** Escribir a StateAlert@taxadmin.org para saber cómo reportar en cada estado donde preparamos declaraciones.
4. **Avisar a las autoridades.** Hacer 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, avisar a la FTC en un plazo de 30 días desde que se descubre.
6. **Avisar a los clientes y al estado.** Según la Ley de Protección de la Información de Florida (Fla. Stat. § 501.171), avisar a los clientes afectados a más tardar 30 días después de descubrir la filtración. Si son 500 floridanos o más, avisar también al Departamento de Asuntos Legales (oficina del Fiscal General) en ese mismo plazo.
7. **Llamar al seguro y al soporte de IT.** Avisar al seguro de ciberseguridad antes de contratar a nadie y pedir ayuda profesional para limpiar los equipos.
8. **Documentar todo.** Fechas, horas, qué pasó, a quién se avisó y qué se cambió. Después, actualizar este plan.

Rosa tiene impresos estos 8 pasos junto a su escritorio. Los contactos están en el Anexo C.

10. Implementación, revisión anual y firma

Luna Tax Services LLC adopta este Plan Escrito de Seguridad de la Información a partir del 15 de diciembre de 2026. Rosa Luna, como Individuo Calificado, es responsable de aplicarlo, de que todo el personal lo conozca y de revisarlo cada diciembre, antes de renovar su PTIN. También se revisa cuando cambian los sistemas, el personal o los proveedores, y después de cualquier incidente.

Fecha	Qué se revisó o cambió	Revisó
15/12/2026	Versión inicial	Rosa Luna

Firma del Individuo Calificado:

Nombre: Rosa Luna

Firma: _____ Fecha: 15 de diciembre de 2026

Dónde se guarda el plan: copia impresa en el gabinete con llave de la oficina y copia digital en la nube cifrada de la oficina.

Anexo A: Acuerdo de confidencialidad y seguridad para el personal

Yo, [nombre de la asistente], que trabajo en Luna Tax Services LLC como asistente de temporada, 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 a Rosa Luna 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 15 de enero de 2027.

Firma: _____ Fecha: _____

Anexo B: Política de documentos para clientes

Cómo protegemos su información en Luna Tax Services

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 3 años y después los destruimos de forma segura.

¿Preguntas? Llámenos al [teléfono].

Anexo C: Contactos de emergencia

Contacto	Para qué	Teléfono o correo
Rosa Luna (Individuo Calificado)	Dirigir la respuesta	[ ]
IRS Stakeholder Liaison de Florida	Reportar el robo de datos de clientes	[ ]
Federación de Administradores Tributarios	Saber cómo reportar a los estados	StateAlert@taxadmin.org
Policía de Kissimmee	Hacer el reporte	[ ]
FBI, oficina de Tampa	Hacer el reporte	[ ]
Técnico de IT	Contener y limpiar los equipos	[ ]
Seguro de ciberseguridad	Abrir el reclamo	[ ]
Proveedor del software de impuestos	Bloquear cuentas y revisar accesos	[ ]
Florida, Departamento de Asuntos Legales	Notificación de filtración (500+ floridanos)	[ ]