Cómo crear un **Plan de seguridad de información escrito** para la seguridad de datos

WISP

Con los continuos incidentes de seguridad de datos, los profesionales de impuestos deben tener planes de seguridad de información escritos o WISPs, por sus siglas en inglés.

La ley federal, aplicada por la Comisión Federal de Comercio (FTC), requiere que los preparadores de impuestos profesionales creen y mantengan un plan de seguridad de información por escrito.

Tener un WISP protege a las empresas y a los clientes, al tiempo que proporciona un plan de acción en caso de un incidente de seguridad. Además, un WISP puede ayudar si ocurren otros eventos que pueden interrumpir seriamente la capacidad de un profesional de impuestos para llevar a cabo negocios normales, incluidos incendios, inundaciones, tornados, terremotos y robos.

La Cumbre de Seguridad desarrolló una muestra del plan en lenguaje sencillo que los profesionales de impuestos pueden usar como guía para hacer su propio WISP. La muestra del plan está disponible en IRS.gov.

Un **plan de seguridad** debe ser adecuado al tamaño de la empresa, al alcance de las actividades, y a la complejidad y sensibilidad de los datos de los clientes que maneja.

Desarrollo de un WISP

Un buen **WISP** debe identificar los riesgos de pérdida de datos para los tipos de información que maneja una empresa y centrarse en tres áreas:

1. Manejo y capacitación de empleados.
2. Sistemas de información.
3. Detección y manejo de fallos del sistema.

Comprender las responsabilidades posteriores a una filtración es importante para crear un WISP. Un buen recurso es la **Guía de Respuesta a la Filtración de Datos de la FTC**.

Como parte del plan, la FTC requiere que cada empresa:

- Designe a uno o más empleados para coordinar su programa de seguridad de la información.
- Identifique y evalúe los riesgos a la información del cliente en cada área relevante de la operación de la empresa y evalúe la efectividad de las medidas de seguridad actuales para controlar esos riesgos.
- Diseñe e implemente un programa de medidas de seguridad, y la monitorice y pruebe regularmente.
- Seleccione proveedores de servicios que puedan mantener las medidas de seguridad adecuadas.
- Evalúe y ajuste el programa tomando en cuenta las circunstancias pertinentes, incluidos los cambios en el negocio o las operaciones de la empresa, o los resultados de las pruebas de seguridad y supervisión.

Mantenimiento de un WISP

Un buen plan de seguridad requiere un mantenimiento regular. Estos son algunos consejos para mantener la eficacia de un WISP:

- Una vez terminado, los profesionales de impuestos deben mantener su WISP en un formato que otros puedan leer fácilmente, como PDF o Word. Se recomienda también poner el WISP a disposición de los empleados con fines de adiestramiento. Almacenar una copia fuera de las instalaciones o en la nube es una práctica recomendada en caso de desastre físico.
- Es importante entender que un WISP está destinado a ser un documento permanente. Es importante revisar y actualizar periódicamente cualquier plan de seguridad, así como ajustar el plan para adaptarlo a los cambios en el tamaño, el alcance y la complejidad del negocio de un profesional de impuestos
- Como parte de un plan de seguridad, el IRS también recomienda a los profesionales de impuestos crear un plan de respuesta al robo de datos, que incluye ponerse en contacto con el Enlace de Partes Interesadas del IRS para informar de un robo. Consulte con los requisitos de respuesta a filtración de datos de la FTC que se mencionan previamente.

Este documento provee una visión general de la Publicación 5708 del IRS. Para información adicional escanee el código QR.

Publication 5709 (sp) (Rev. 5-2024) Catalog Number 94993K Department of the Treasury **Internal Revenue Service** www.irs.gov