Lista de Verificación para **Crear un Plan de Seguridad**

La Regla de Salvaguardias requiere que las empresas evalúen y aborden los riesgos para la información del cliente en todas las áreas de su operación, incluidas tres áreas que son particularmente importantes para la seguridad de la información: Gestión y Capacitación de Empleados; Sistemas de información; y Detección y gestión de fallas del sistema.

No todas estas recomendaciones se aplicarán a las circunstancias que se encuentran en las oficinas de los preparadores de impuestos, pero aún brindan los componentes básicos para la creación de un plan de seguridad y reforzar las recomendaciones del IRS de que los profesionales de impuestos establezcan protocolos de seguridad sólidos. Dependiendo de la naturaleza de sus operaciones comerciales, las empresas deben considerar implementar las siguientes prácticas:

Manejo de Empleados y Entrenamiento

	ONGOING	DONE	N/A
El éxito de su plan de seguridad de la información depende en gran medida de los empleados quienes lo implementan. Considere estos pasos:	☐	☐	☐
Verifique las referencias y los antecedentes antes de contratar empleados que tendrán acceso a la información del cliente.	☐	☐	☐
Solicite a cada nuevo empleado que firme un acuerdo para seguir las normas de confidencialidad y seguridad para el manejo de la información de los clientes.	☐	☐	☐
Limitar el acceso a la información del cliente a los empleados que tengan un motivo comercial para verlo. Por ejemplo, dé a los empleados que responden a las consultas de los clientes acceso a los archivos de los clientes, pero solo en la medida en que lo necesiten para hacer su trabajo.	☐	☐	☐
Controle el acceso a la información confidencial exigiendo a los empleados que usen contraseñas "fuertes" que deben cambiarse periódicamente. (Difícil de romper las contraseñas requieren el uso de al menos seis caracteres, mayúsculas y minúsculas letras y una combinación de letras, números y símbolos). (Consejo del IRS: las contraseñas deben tener un mínimo de ocho caracteres, de acuerdo a los estándares del NIST (Instituto Nacional de Estándares y Tecnología. No permita el uso compartido de contraseñas; asegurese que cada empleado que tenga acceso a cuentas de los contribuyentes utiliza una contraseña única.)	☐	☐	☐
Use protectores de pantalla activados de contraseñas para bloquear las computadoras de los empleados después de un período de inactividad.	☐	☐	☐
Desarrolle políticas para el uso adecuado y protección de computadoras portátiles, asistentes personal digital, teléfonos u otros dispositivos móviles. Por ejemplo, asegúrese de que los empleados guarden estos dispositivos en un lugar seguro cuando no estén en uso. Además, tenga la información del cliente en archivos encriptados, estarán mejor protegidos en caso de robo de tal dispositivo.	☐	☐	☐
Capacite a los empleados para que tomen medidas básicas para mantener la seguridad, confidencialidad y la integridad de la información del cliente, que incluyen:	☐	☐	☐
• Oficinas aseguradas y archivadores protegidos donde se guardan los registros;	☐	☐	☐
• No comparta ni publique abiertamente las contraseñas de los empleados en las áreas de trabajo;	☐	☐	☐
• Encriptar la información confidencial del cliente cuando se transmite electrónicamente a través de redes públicas;	☐	☐	☐
• Referir llamadas u otras solicitudes de información del cliente a personas designadas que hayan recibido capacitación sobre cómo su empresa protege los datos personales; y	☐	☐	☐
• Reportar intentos sospechosos de obtener información del cliente a personal designado.	☐	☐	☐

	ONGOING	DONE	N/A
Recuerde frequentemente a todos los empleados la política de su empresa y los requisitos legales para mantener la información del cliente segura y confidencial. Por ejemplo, considere publicar recordatorios sobre su responsabilidad por la seguridad en las áreas donde se almacena la información del cliente, como las salas de archivos.	☐	☐	☐
Desarrollar políticas para los empleados que realicen teletrabajo. Por ejemplo, considere si se debe permitir que los empleados mantengan o accedan a los datos de los clientes en casa y cómo hacerlo. Además, exija a los empleados que usan computadoras personales que guardan o acceden a datos de clientes que usen protecciones contra virus, spyware (programa espía) y otras intrusiones no autorizadas.	☐	☐	☐
Imponer medidas disciplinarias por violaciones a la política de seguridad.	☐	☐	☐
Evite que los empleados despedidos accedan a la información del cliente desactivando inmediatamente sus contraseñas y nombres de usuario y tomando otras medidas apropiadas. (Consejo del IRS: desactive el acceso antes del despido).	☐	☐	☐
(Consejo del IRS: Agregue etiquetas a los documentos para indicar su importancia, como "Sensible" o "Para asuntos oficiales" para proteger aún más los documentos en papel.	☐	☐	☐

Sistemas de Información

Los sistemas de información incluyen el diseño de redes y software, y el procesamiento, almacenamiento, transmisión, recuperación y eliminación de información. Estas son algunas sugerencias de la FTC para mantener la seguridad a lo largo del ciclo de vida de la información del cliente, desde la entrada de datos hasta su eliminación:

Conozca dónde se guarda la información confidencial de los clientes y tengala de forma segura. Asegúrese de que solo los empleados autorizados tengan acceso. Por ejemplo:	☐	☐	☐
• Asegúrese de que las áreas de almacenamiento estén protegidas contra la destrucción o el daño causado por peligros físicos, como incendios o inundaciones.	☐	☐	☐
• Cuando la información del cliente se almacena en un servidor u otra computadora, asegúrese de que la computadora sea accesible solo con una contraseña "fuerte" y se mantenga en un área físicamente segura. • **(Consejo del IRS: si usa un servicio de almacenamiento en la nube, use una contraseña segura, opciones de autenticación de múltiples factores y tenga cuidado con los ladrones haciéndose pasar por proveedores).**	☐	☐	☐
• Siempre que sea posible, evite almacenar datos confidenciales de los clientes en una computadora con conexión a Internet.	☐	☐	☐
• Mantenga registros de respaldo protegidos y mantenga seguros los datos archivados almacenándolos fuera de línea y en un área físicamente segura.	☐	☐	☐
• Mantenga un inventario cuidadoso de las computadoras de su empresa y cualquier otro equipo en el que se pueda guardar la información del cliente.	☐	☐	☐
Tome medidas para garantizar la transmisión segura de la información del cliente. Por ejemplo:	☐	☐	☐
• Cuando transmita información de tarjetas de crédito u otros datos financieros confidenciales, use niveles de puertos seguros (SSL) u otra conexión segura, para que la información esté protegida en tránsito. **Consejo del IRS: Seguridad de la capa de transporte 1.3 es la más nueva y segura**	☐	☐	☐
• Si recopila información en línea directamente de los clientes, haga que la transmisión segura sea automática. Advierta a los clientes sobre la transmisión de datos confidenciales, como números de cuenta, por correo electrónico o la respuesta a un correo electrónico o mensaje de emergencia no solicitado.	☐	☐	☐
• Si debe transmitir datos confidenciales por correo electrónico a través de la Internet, asegúrese de encriptar los datos. **(Consejo del IRS: en lugar de usar el correo electrónico, transmita los archivos a través del Protocolo seguro de transferencia de archivos (SFTP), sucesor del Protocolo de transferencia de archivos (FTP)).**	☐	☐	☐

	ONGOING	DONE	N/A
Elimine la información del cliente de manera segura y, cuando corresponda, de conformidad con la Regla de eliminación de la FTC. Por ejemplo:	☐	☐	☐
• Considere la posibilidad de designar o contratar a un administrador de retención de registros para supervisar la eliminación de los registros que contienen información del cliente. Si contrata a una empresa de eliminación externa, realice la debida diligencia de antemano verificando las referencias o exigiendo que la empresa esté certificada por un grupo industrial reconocido.	☐	☐	☐
• Queme, pulverice o triture papeles que contengan información del cliente para que la información no se pueda leer ni reconstruir.	☐	☐	☐
• Destruir o borrar datos al desechar computadoras, discos, CD, cintas magnéticas, discos duros, computadoras portátiles, PDA, teléfonos celulares o cualquier otro medio electrónico o hardware que contenga información del cliente.	☐	☐	☐

Detectar y Manejar Fallas en el Sistema

La gestión eficaz de la seguridad requiere que su empresa impida, detecte y se defienda contra las infracciones de seguridad. Eso significa tomar medidas razonables para prevenir ataques, diagnosticar rápidamente un incidente de seguridad y tener un plan para responder de manera efectiva. Considere implementar los siguientes procedimientos:

Supervise los sitios web de sus proveedores de software y lea publicaciones relevantes de la industria para obtener noticias sobre amenazas emergentes y defensas disponibles.	☐	☐	☐
Mantener programas y controles actualizados y apropiados para evitar el acceso no autorizado a la información del cliente. Asegúrese de:	☐	☐	☐
• Revisar regularmente con los proveedores de software para obtener e instalar parches que resuelvan las vulnerabilidades del software;	☐	☐	☐
• utilizar software antivirus y antispyware que se actualice automáticamente;	☐	☐	☐
• mantener actualizados los cortafuegos, especialmente si utiliza una conexión a Internet de banda ancha o permite que los empleados se conecten a su red desde su hogar u otras ubicaciones fuera del sitio;	☐	☐	☐
• asegúrese regularmente de que los puertos que no se utilizan para su negocio estén cerrados; y	☐	☐	☐
• transmitir de inmediato información e instrucciones a los empleados sobre cualquier nuevo riesgo de seguridad o posibles infracciones.	☐	☐	☐
Utilice procedimientos de supervisión o auditoría adecuados para detectar la divulgación indebida o el robo de información del cliente. Sea sabio al:	☐	☐	☐
• mantener registros de actividad en su red y supervisarlos en busca de signos de acceso no autorizado a la información del cliente;	☐	☐	☐
• usar un sistema actualizado de detección de intrusos para alertarlo de ataques;	☐	☐	☐
• supervisar las transferencias de información entrantes y salientes en busca de indicios de compromiso, como la transmisión inesperada de grandes cantidades de datos desde su sistema a un usuario desconocido; y	☐	☐	☐
• inserte una cuenta ficticia en cada una de sus listas de clientes y controle la cuenta para detectar contactos o cargos no autorizados.	☐	☐	☐

	ONGOING	DONE	N/A
Tome las medidas para preservar la seguridad, la confidencialidad y la integridad de la información del cliente en caso de incumplimiento. Si se produce una infiltración:	☐	☐	☐
• tomar medidas inmediatas para proteger cualquier información que haya sido o pueda haber sido comprometida. Por ejemplo, si una computadora conectada a la Internet está comprometida, desconéctela de la Internet;	☐	☐	☐
• conservar y revisar archivos o programas que puedan revelar cómo la violación a la seguridad ocurrió; y	☐	☐	☐
Considere notificar a los consumidores, las agencias del orden y/o las empresas en caso de una violación de la seguridad. Por ejemplo:	☐	☐	☐
• notificar a los consumidores si su información personal está sujeta a una violación que presenta un riesgo significativo de robo de identidad o daño relacionado;	☐	☐	☐
• notificar a las agencias del orden público si la infracción puede implicar una actividad delictiva o si hay pruebas de que la infracción ha resultado en un robo de identidad o un daño relacionado;	☐	☐	☐
• notificar a las agencias de crédito y otras empresas que puedan verse afectadas por el incumplimiento. Consulte la Guía de Compromiso y Riesgo del Robo de Identidad para su empresa; y	☐	☐	☐
• verifique si la ley estatal requiere la notificación del incumplimiento.	☐	☐	☐
• (Consejo del IRS: los profesionales que experimentan una pérdida de datos deben comunicarse con el IRS y los estados. Además, considere tener un contrato de soporte técnico vigente, de modo que los eventos del disco duro-hardware- puedan repararse en un tiempo razonable y con una interrupción mínima de la disponibilidad del negocio.)	☐	☐	☐