# Controles sobre el cumplimiento federal
# Agosto de 2025

IL T&TA
INDEPENDENT LIVING
TRAINING AND TECHNICAL ASSISTANCE CENTER

Presentadores:
John Heveron, Jr., Contador Público (CPA)
Paula L. McElwee

# **Antes de comenzar:** accesibilidad

- Los intérpretes de Lengua de Señas Americana (ASL) y español están disponibles e identificados.
- Para acceder a los subtítulos, haga clic en el botón “CC” ubicado en la parte inferior de la ventana de Zoom.
- Para hacer preguntas, utilice las funciones de levantar la mano o el chat de Zoom.
- Recuerde mencionar su nombre antes de hablar.
- Envíe un mensaje a nuestro equipo de IL T&TA a través del chat si tiene dificultades con la llamada de hoy.
- Complete la encuesta al final de la capacitación.

# Contenidos

- **Los requisitos para los controles sobre los fondos federales**
- **Cómo documentar los controles y asegurarse de que se sigan**
- **Entender cómo los controles internos garantizan el cumplimiento de los requisitos federales**
- **Cómo protegerse de las amenazas cibernéticas**

# Contenidos

**Paula McElwee**

Directora de Asistencia Técnica

Centro IL T&TA

**John Heveron, Jr., CPA**

Consultor del Centro IL T&TA

Director de Heveron y Compañía CPAs

# Controles sobre el cumplimiento federal

Los objetivos de los controles sobre el cumplimiento incluyen los siguientes:

- Garantizar que los estados financieros y los informes federales estén debidamente preparados y sean precisos.
- Garantizar que los procesos fiscales clave tengan los controles y balances oportunos.
- Hacer un seguimiento y proteger los activos.
- Demostrar que está siguiendo las reglas federales y los términos de la concesión.
- Proteger la información personal y confidencial.

# Requisitos de cumplimiento que pueden influir directamente en sus programas

Las posibles áreas de cumplimiento requerido incluyen las siguientes:

- Fuentes de financiamiento específicas, incluidos los números de concesión.
- Qué actividades están o no permitidas.
- Qué gastos son aceptables.
- Gestión de efectivo (cronograma y documentación de retiros).
- Elegibilidad de las personas atendidas.
- Requisitos de compatibilidad.
- Período de rendimiento.
- Informes requeridos.

# Requisitos de cumplimiento que pueden influir directamente en sus programas (cont.)

- No todas las áreas anteriores se aplican a todas las fuentes de financiamiento, aunque, en general, se aplicará la mayoría, como actividades permitidas o no permitidas, gastos aceptables/principios de gastos, gestión de efectivo, elegibilidad y período de rendimiento.
- Cuando cualquiera de estas áreas se aplica y son **directas** e **importantes**, deberá tener (y documentar que tiene) controles sobre esas áreas.
  - Directas: claramente atribuible a una transacción, cuenta o actividad específica.
  - Importante: lo suficientemente significativa como para influir en decisiones, resultados o exposición al riesgo.
- ¿Siempre sabe a qué concesión está aplicando gastos y es consistente? Debería.

# Revisión integral de los requisitos de control interno generales

1. ¿Tiene el beneficiario el personal, los sistemas y los procesos adecuados para ofrecer una garantía razonable de que los premios de la Administración para la Vida Comunitaria (ACL) se utilizan de acuerdo con las leyes, estatutos, regulaciones y términos y condiciones aplicables?
2. ¿Tiene la junta del Centro para la Vida Independiente (CIL) responsabilidades de control interno claramente definidas y se están implementando de manera consistente?
3. ¿Están adecuadamente separadas las funciones y responsabilidades para garantizar que los procesos fiscales clave tengan controles y equilibrios adecuados?
4. ¿Están codificados los procesos y procedimientos fiscales en la política del beneficiario? ¿Está la política actualizada?
5. ¿Tiene el beneficiario un proceso interno de revisión o evaluación para evaluar el cumplimiento de sus propias políticas y procesos?
6. ¿Tiene el beneficiario políticas sobre modificaciones presupuestarias y se están implementando de manera consistente?

Fuente: Lista de verificación de revisión fiscal de programas de concesiones de ACL IL

# Ejemplos de controles internos

Los controles específicos sobre las actividades permitidas y los gastos aceptables/principios de gastos deben incluir elementos como los siguientes:

- Revisión de contratos por una persona experta en la materia para identificar actividades permitidas, el presupuesto general, si ciertos gastos o actividades requieren aprobación previa.

Los controles específicos sobre la gestión de efectivo podrían incluir lo siguiente:

- Revisión del contrato para determinar el método de retiro y evaluar el proceso para documentar los retiros.
- Desarrollo de un sistema de informes para identificar cualquier error entre los retiros y los desembolsos.

# Ejemplos de controles internos (cont.)

- Los controles específicos del período de rendimiento podrían incluir lo siguiente:
  - Revisión de contratos para identificar cuándo se pueden realizar los servicios y cualquier requisito único sobre el gasto previo a la adjudicación, extensiones y reembolso de montos no utilizados.
  - Revisión del plan de programa de tres años y la garantía de que está gastando fondos federales de acuerdo con el propósito de los fondos de vida independiente.

# Directrices sobre controles internos

En la Parte 6 del Anexo de Cumplimiento 2024 se brindan directrices sobre los controles internos. Se enfatiza que el control interno debe cumplir con las directrices del Comité de Organizaciones Patrocinadoras (COSO) y el Libro Verde. COSO es el Comité de Organizaciones Patrocinadoras, organizaciones de liderazgo contable y financiero, y el Libro Verde abarca controles internos para entidades gubernamentales. Ambos son similares e identifican 5 áreas clave de control y 17 principios.

# 5 áreas clave de control interno

1. Entorno de control: compromiso con la integridad y los valores éticos; supervisión y compromiso con la competencia y la responsabilidad (la capacitación continua es importante).
2. Evaluación de riesgos: identificación y análisis de riesgos, y evaluación de riesgos de fraude.
3. Actividades de control: políticas y procedimientos que se adoptan para la contabilidad y documentación, y controles sobre la tecnología.

# 5 áreas clave de control interno (cont.)

4. Información y comunicación: comunicación y capacitación internas y comunicación externa sobre políticas, procedimientos y valores.
5. Actividades de supervisión: evaluación continua para garantizar que los controles son apropiados para sus programas actuales y que se están siguiendo.

# Actividades de control

- Cuando se trata de controles internos, ya sea a nivel de agencia o específicamente relacionados con una concesión o contrato: **si no lo documenta, no lo hizo.**
- Esto se aplica tanto al establecer un entorno de control adecuado como al realizar la evaluación de riesgos, establecer actividades de control, comunicar procedimientos, políticas y actividades de control, y al supervisar.
- Los auditores independientes que realizan auditorías de cumplimiento están obligados a revisar sus controles sobre el cumplimiento y los auditores de la ACL y otros financiadores también lo harán.

# Actividades de control (cont.)

- Es probable que esté realizando ciertas actividades de supervisión, como el desarrollo de presupuestos y comparación de resultados presupuestados con los reales, evaluación de seguros/riesgos, revisión de deudores/acreedores, control de liquidez y discusión de controles de efectivo.
- Hay varias otras medidas que puede tomar para supervisar los controles: revíselas y analícelas (posiblemente, en un comité ejecutivo o de finanzas), seleccione algunas y documente la selección y el análisis así como la ejecución de los procedimientos que seleccione.
- Puede supervisar diferentes áreas, como las que se indican a continuación, de manera rotativa, quizás abarcando cada área cada tres años.

# Posibles procedimientos de supervisión

- Revisar el proceso de contratación, archivos de personal o supervisión de nómina salarial.
- Revisar la precisión e integridad de las comunicaciones de recaudación de fondos.
- Verificar que las cuentas bancarias se concilien de manera oportuna.
- Revisar el proceso de compras.
- Evaluar la seguridad física de la información confidencial.
- Revisar la documentación de tarjetas de cargo y los reembolsos de gastos.
- Evaluar el proceso de capacitación del personal.
- Preguntar al personal si su capacitación y mentoría son suficientes.

El personal remoto o parcialmente remoto puede requerir algunos cambios en sus procedimientos de supervisión.

# Los CIL y SILC son responsables de la seguridad

- Los “datos individualmente identificables” son datos que identifican a la persona de la que se trata la información.
- La “información de salud individualmente identificable” es información de salud personal protegida por HIPAA y otras regulaciones.
- Los CIL y SILC deben tomar medidas para limitar los riesgos de seguridad cibernética.
- Los CIL y SILC deben tomar todas las medidas razonables para proteger la confidencialidad de esta información.

# Los CIL y SILC son responsables de la seguridad (cont.)

- Es decir, la seguridad física y técnica de la información de empleados y consumidores.
- Significa limitar el acceso y probar la seguridad, posiblemente mediante sistemas de detección de intrusiones.
- Un plan de recuperación de desastre informático puede aumentar la seguridad.

# Riesgos de seguridad cibernética

- Las empresas y organizaciones sin fines de lucro son hackeadas todos los días.
- El grupo que supervisa por video las comitivas presidenciales fue hackeado al azar por una pareja en Europa Oriental.
- En el informe más reciente de la Asociación de Examinadores de Fraude Certificados "*Informe a las Naciones*" se confirman importantes violaciones de seguridad cibernética, incluidas las de organizaciones sin fines de lucro. https://legacy.acfe.com/report-to-the-nations/2024/
- Veamos algunos recursos para evitar pasar por la misma situación.

# Riesgos de seguridad cibernética (cont.)

- ¿Qué quieren los cibercriminales? Dinero de sus cuentas, dinero de rescate (secuestro), números de tarjetas de crédito, números de Seguro Social (que pueden vender por dinero).
- ¿Qué están dispuestos a hacer para conseguirlo? Están dispuestos a pasar toda su vida tratando de engañarlo y robarle: todo el día, todos los días. Y están bien pagados.
- ¿Cómo se pueden reducir los hackeos de la seguridad cibernética en un 90 %?

# Seguridad sobre cuentas financieras

Los cheques falsificados y los secuestros de cuentas bancarias pueden reducirse con contramedidas tecnológicas, como las siguientes:

- Cheques seguros.
- Pago positivo (proporcionar al banco información sobre los cheques que ha emitido para su control).
- Pago positivo inverso (revisar los cheques entrantes antes de que sean procesados).
- Uso de una fuente segura y uso de asteriscos sobre el nombre del beneficiario para evitar la adición de otro nombre.

# Seguridad de cuentas financieras (cont.)

- Nunca proporcione información confidencial al banco a menos que usted inicie la llamada.
- No responda a una solicitud de correo electrónico de un banco haciendo clic en un hipervínculo.
- Busque el https://protocol en sitios web bancarios y otros.

# Seguridad informática

- Los servidores y estaciones de trabajo solo deben usar sistemas operativos que sean actualmente compatibles: la compatibilidad de Windows 10 finaliza el 14 de octubre de 2025.
- Las actualizaciones y parches del sistema operativo deben instalarse de inmediato.
- Las copias de seguridad deben almacenarse en una ubicación externa o en la nube con suficiente frecuencia para evitar una pérdida significativa de datos.

# Seguridad informática (cont.)

- La formación en informática y seguridad informática debe ofrecerse en varios momentos a lo largo del año. Incluir concienciación sobre la seguridad cibernética e ingeniería social (reconocer y evitar archivos adjuntos de correo electrónico peligrosos, descargas dudosas y mensajes de voz falsos).
- Las estaciones de trabajo deben configurarse para cerrar sesión automáticamente después de determinado tiempo.

# Seguridad informática (cont. 2)

- Las copias de seguridad deben verificarse periódicamente para asegurarse de que están funcionando.
- Todas las computadoras deben tener protectores contra sobretensiones y los servidores deben tener copias de seguridad de UPS/batería correctamente configuradas.
- El acceso a los programas debe limitarse según la necesidad de acceso.
- El acceso debe ser revocado para cualquier persona que se vaya o sea despedida.

# Seguridad informática (cont. 3)

- Los discos duros deben desfragmentarse periódicamente.
- La información de licencias y garantías debe mantenerse en un lugar central seguro.
- Considere seriamente contar con una organización externa para la supervisión remota continua y para actualizaciones y problemas.

# Defensa de seguridad cibernética

- Capacite a su personal en concienciación sobre la seguridad cibernética.
- Recuerde periódicamente al personal sobre las amenazas, riesgos y el impacto potencial de los ciberataques.
- Incluya la seguridad cibernética como parte de las reuniones del personal.
- Aquí puede encontrar un video y algunas pautas sobre cómo reducir los ataques a la seguridad cibernética.
- https://www.youtube.com/playlist?list=PLmvQaMcWIqbtQp81nL_g63NlOqzRRkTds Consejos de seguridad de 45 segundos con subtítulos.
- Consejos cortos del día. https://inspiredelearning.com/resource/security-awareness-tip-day/

# Defensa de la seguridad cibernética (cont.)

- El Marco de Seguridad Cibernética del Instituto Nacional de Estándares (NIST) brinda una base para construir o mejorar un programa de seguridad cibernética.
- El marco incluye cinco funciones: **identificar, detectar, responder, proteger y recuperar.**
- **Identificar** implica identificar a todas las personas, dispositivos y programas que puedan acceder a nuestros sistemas.
- **Detectar** implica actividades que nos permiten detectar eventos de seguridad cibernética de manera oportuna.

# Defensa de la seguridad cibernética (cont. 2)

- Los tres objetivos de la seguridad de la información incluyen **confidencialidad, integridad** y **disponibilidad**.
- **Confidencialidad** para proteger datos sensibles o restringidos de accesos o divulgaciones no autorizadas.
- **Integridad** para mantener la precisión, totalidad y consistencia de los datos durante su ciclo de vida.
- **Disponibilidad** para asegurar que los usuarios autorizados tengan acceso oportuno e ininterrumpido a los recursos y servicios que necesitan.

# Defensa de la seguridad cibernética (cont. 3)

- **Responderemos** de inmediato a los incidentes de seguridad cibernética, incluyendo un análisis.
- **Protección:** cada servidor, computadora y dispositivo móvil conectado debe tener un software antivirus y antimalware instalado y funcionando en tiempo real. Esto incluye dispositivos internos así como cualquier remoto u otros que tengan acceso.
- **Recuperación:** mediante la restauración del acceso normal, incluida la eliminación de cualquier acceso no autorizado y restauración rápida desde copias de seguridad.

# Defensa de la seguridad cibernética (cont. 4)

- Los puntos de acceso inalámbricos deben estar asegurados con contraseñas y los clientes/invitados solo tendrán acceso a puntos de acceso inalámbricos separados.
- Los empleados nunca deben hacer clic en el botón “ok” en ventanas emergentes. Podrían descargar malware. Para cerrar ventanas emergentes, haga clic en la X en la esquina superior derecha o presione “Ctrl-W”.
- Desactive la función “AutoRun/autoplay” que ejecuta automáticamente el contenido en un CD/DVD/unidad USB.
- Cuando esté disponible, active la autenticación en dos pasos.

# Defensa de la seguridad cibernética (cont. 5)

- Cuando los empleados se vayan, de manera voluntaria o de otro modo, los dispositivos de propiedad de la empresa deberán devolverse y el acceso a la cuenta deberá cerrarse en el momento de la salida.
- A los hackers les gusta poner códigos maliciosos en unidades USB y colocarlos en áreas donde los empleados podrían encontrarlos. Nunca conecte unidades USB externas.
- La eliminación de computadoras, fotocopiadoras y otros dispositivos físicos que pueden contener información confidencial debe realizarse adecuadamente a través de una empresa de eliminación certificada. Obtenga un certificado de destrucción para estos dispositivos. Los dispositivos como CD y USB deben destruirse físicamente.

# Preguntas

# Recursos

- Considere comunicarse con una empresa de seguridad informática. Incluso si elige no contratarla, podría obtener algún beneficio de sus recomendaciones.
- El Marco de Seguridad Cibernética del NIST ofrece orientación y recursos para la seguridad cibernética. https://www.nist.gov/cyberframework.
- En https://www.techsoup.org/ también encontrará recursos de seguridad e informáticos útiles.
- El centro de gestión del riesgo sin fines de lucro tiene recursos contra riesgos en https://nonprofitrisk.org/.
- El marco de control interno del COSO se puede encontrar en https://www.coso.org/internal-control.
- El formato de control interno del Libro Verde se puede encontrar en https://www.gao.gov/products/gao-14-704g.
- Lista de verificación de revisión fiscal de programas de concesiones de la ACL IL https://acl.gov/sites/default/files/programs/2024-12/ACL%20IL%20Grant%20Programs%20Fiscal%20Review%20Checklist%20-%20Published%2012.10.2024.docx

# Evaluación

Gracias por participar en la capacitación de hoy.

Su opinión nos importa. Utilice el enlace en el chat para compartir sus comentarios.

# Información de contacto


## Centro de Capacitación y Asistencia Técnica para la Vida Independiente

Instituto Rural para Comunidades Inclusivas de la Universidad de Montana

📞 (406) 243-5300

✉️ ilttacenter@mso.umt.edu

🌐 www.ILTTACenter.org

👉 Manténgase conectado Inscripción por correo electrónico | Facebook | LinkedIn | Instagram



*El Centro de Capacitación y Asistencia Técnica para la Vida Independiente colabora con la Administración para la Vida Comunitaria del Departamento de Salud y Servicios Humanos de los EE. UU.*

# Centro de Capacitación y Asistencia Técnica para la Vida Independiente

El Centro de Capacitación y Asistencia Técnica para la Vida Independiente (Centro IL T&TA) está disponible para usted a través de un **contrato con el Departamento de Salud y Servicios Humanos de los EE. UU**.

El Centro IL T&TA ofrece **formación de expertos y asistencia técnica** a los Centros para la Vida Independiente (CIL), Consejos Estatales de Vida Independiente (SILC) y Entidades Estatales Designadas (DSE).

El Centro es operado por el **Instituto Rural para Comunidades Inclusivas** de la Universidad de Montana.

UNIVERSITY OF MONTANA

IL T&TA
INDEPENDENT LIVING
TRAINING AND TECHNICAL ASSISTANCE CENTER