Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

Reunión de validación virtual de la CTPAT

* Le informamos que esta es una agenda de muestra y se emplea como guía para abordar y prepararse para una validación de la CTPAT. Dado que la agenda no representa a todas las entidades y su criterio de seguridad mínima (*Minimum-Security Criteria*, MSC), es responsabilidad del socio de la CTPAT revisar todos los MSC correspondientes para que su respectiva entidad garantice el cumplimiento.

La validación virtual: el proceso de validación virtual utiliza la conferencia de video para conectar de manera segura a socios de la Asociación Comercial Aduanera contra el Terrorismo (Customs Trade Partnership Against Terrorism, CTPAT) y a sus representantes con el especialista en Seguridad de la Cadena de Suministro (*Supply Chain Security Specialist*, SCSS) asignado, y permite intercambio, revisión y validación seguros de datos de seguridad pertinentes de la cadena de suministro en un entorno en tiempo real. En la medida de lo posible, la validación virtual reflejará el proceso de validación física e incluirá una revisión de la documentación escrita, los procedimientos y las medidas de seguridad que se implementan para garantizar la cadena de suministro internacional del socio de la CTPAT. En función de las capacidades técnicas, se puede llevar a cabo una revisión de requisitos críticos de los criterios de seguridad mínima (MSC) para incluir la seguridad física de la instalación mediante la plataforma de conferencias de video.

* El proceso de validación incluye la verificación del cumplimiento de los MSC de la CTPAT por parte del socio de la CTPAT. El proceso de validación básicamente se basa en (y requiere) **políticas empresariales por escrito** que rigen la seguridad de la cadena de suministro y la **evidencia de implementación** para las políticas de seguridad de la empresa.

Los procedimientos operativos estándares (*standard operating procedures*, SOP) por escrito se deben personalizar para adaptarse al modelo de negocio internacional de la empresa. Los SOP se deben escribir en un formato de procedimiento paso a paso para incluir el detalle descriptivo y demostrar, de manera clara, los procedimientos activos y operativos de seguridad del cargamento.

La reunión de validación de la CTPAT es la oportunidad de la empresa de demostrar procesos y prácticas de seguridad normativos relacionados con la función o responsabilidad de la empresa dentro de la cadena de suministro del socio de la CTPAT para envíos con destino a los EE. UU. (p. ej., fabricación de cargamento, transporte de mercancías, almacenamiento y distribución, corretaje o importación).

Las reuniones de validación generalmente duran entre cuatro y seis horas, según la preparación de la empresa y otros factores. Los representantes adecuados de la empresa deben estar disponibles/de guardia para responder preguntas relacionadas con su área de experiencia y responsabilidad, aunque no necesitan asistir a la reunión.

Las siguientes secciones de los MSC de la CTPAT (a continuación) se abordarán en la reunión de Validación a medida que se relacionan con la función de la empresa o la responsabilidad dentro de la cadena de suministro del socio de la CTPAT, con un enfoque en envíos con destino a los EE. UU.

Las principales áreas de enfoque son las siguientes: (1) documentación (SOP) que respalda y demuestra el cumplimiento de la empresa de los MSC de la CTPAT; (2) *detallado en el enlace web de los MSC de*

la CTPAT (a continuación); y (3) descrito en más profundidad en *cada* sección de los MSC a continuación.

La información de los MSC de la CTPAT se detalla en este enlace (en inglés y otros idiomas):
Criterios de seguridad mínima y directrices de la CTPAT

Después de las presentaciones de representantes de la empresa y de la CTPAT, la reunión de validación comenzará con un debate centrado en el modelo de negocio de la empresa y, a continuación, conducirá a un debate y a una revisión de las medidas de seguridad que la empresa implementó en sus operaciones diarias.

Posteriormente a la revisión de las medidas de seguridad de la empresa, el SCSS puede realizar un recorrido "virtual" de la instalación para observar visualmente los procedimientos de seguridad física. La reunión finalizará con un breve debate de cierre y una revisión de los hallazgos por parte del equipo de validación de la CTPAT. Si los procesos y las prácticas de seguridad no se implementan en algún área clave, el equipo analizará posibles soluciones para cumplir con los MSC de la CTPAT, conforme se indica en el enlace anterior y se describe más abajo.

Las secciones de los MSC a continuación describen las medidas de conformidad con la CTPAT que se revisan.

* En la medida de lo posible, la reunión de validación será más productiva si la empresa cuenta con *todos los documentos y los SOP (enumerados a continuación, según corresponda)* disponibles para revisión durante la reunión *

* *Puede utilizar esta Agenda de reunión como directriz para insertar/incluir (en formato electrónico) el ícono de los SOP o del documento correspondiente (.doc o .pdf) en cada sección con viñetas adecuadas. Solo debe hacer clic en el área en la que desea insertar su SOP, hacer clic en "Insertar" en la parte superior izquierda del encabezado y, luego, hacer clic en "Objeto" en la parte superior derecha del encabezado. Aparecerá la casilla "Objeto". Haga clic en "Crear desde archivo", marque la casilla "Mostrar como ícono" y haga clic en "Examinar". Haga doble clic en el SOP o documento que desea insertar y haga clic en "Aceptar".*

- **Seguridad corporativa: Visión de seguridad y responsabilidad**

Esté preparado para analizar el respaldo de la alta gerencia al programa de seguridad de la cadena de suministro de la CTPAT, como también al proceso de auditoría interna de la empresa.

– La administración de la empresa (o el equipo de la CTPAT designado) debe contar con una supervisión activa del programa de seguridad de la empresa y de la cuenta del Portal de la CTPAT.
– La administración de la empresa (o el equipo de la CTPAT designado) debe estar al tanto de los requisitos de la CTPAT.
– El programa de seguridad de la empresa de la CTPAT debe estar respaldado por un componente de revisión por escrito (es decir, los SOP para auditorías/actualizaciones de las políticas y procedimientos de seguridad por escrito de la empresa).

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

– El programa de seguridad de la CTPAT de la empresa debe estar respaldado por una Declaración de soporte.

* La documentación que detalla y demuestra la visión de seguridad, los procedimientos de responsabilidad de la empresa y el proceso de auditoría interna de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad corporativa: Evaluación de riesgos**

Esté preparado para analizar el proceso de evaluación de riesgos (*risk assessment*, RA) de la empresa.

– La empresa debe llevar a cabo una evaluación de riesgo general para identificar vulnerabilidades en la seguridad.
– La empresa debe realizar y documentar el nivel de riesgo en sus cadenas de suministro internacionales.
– La evaluación de riesgo de la empresa se debe respaldar mediante un SOP por escrito (que detalla el proceso de la RA).
– La empresa debe seguir el proceso de evaluación de riesgos de 5 pasos de la CTPAT.
– La evaluación de riesgos debe incluir un proceso documentado de asignación de cargamento/envío.

* La documentación que detalla/demuestra el proceso de evaluación de riesgos de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad corporativa: socios comerciales**

Esté preparado para analizar el proceso de análisis de los Socios comerciales de la empresa.

– La empresa debe contar con un SOP por escrito que documente el proceso basado en riesgos para analizar a los nuevos socios comerciales y monitorear a sus socios comerciales actuales.
* Con base en el modelo de negocio internacional de la empresa y la función o responsabilidad de la empresa en la cadena de suministro del socio de la CTPAT *

– El proceso de análisis debe incluir a socios comerciales clave de la empresa.
* Los socios comerciales clave se designan con base en la esencialidad de su función o responsabilidad dentro de la cadena de suministro. Entre los socios comerciales clave, se incluye a los involucrados en la fabricación, seguridad o facilitación de cargamento/envíos con destino a los EE. UU. (p. ej., proveedores y suministradores [no suministradores de materia prima], proveedores de servicios de logística y transporte, agentes de transporte, guardias de seguridad y agentes de aduanas).

– El SOP de análisis por escrito de la empresa que documenta el proceso se debe estructurar para identificar factores de riesgo específicos (p. ej., indicadores de advertencia/señales de alerta, procedimientos de seguridad no conformes, certificación de la CTPAT o del AEO).
* La documentación que detalla/demuestra el proceso de análisis y auditoría de socios comerciales de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

- **Seguridad corporativa: Ciberseguridad**

Esté preparado para analizar los procedimientos y las políticas de ciberseguridad de la empresa.

– La empresa debe implementar un SOP por escrito para procedimientos y políticas de ciberseguridad, para proteger los sistemas informáticos de la empresa.
– El SOP de ciberseguridad/TI de la empresa se debe revisar y actualizar, al menos, una vez al año.
– El SOP de ciberseguridad/TI de la empresa debe incluir procedimientos para evitar ataques a través de ingeniería social.
– La empresa debe capacitar a los empleados relevantes con respecto a las políticas y los procedimientos de ciberseguridad/TI.
– Los empleados de la empresa que gestionan los sistemas de tecnología de ciberseguridad/seguridad de TI deben recibir capacitación.
– La empresa debe documentar la capacitación recibida por los empleados (p. ej., ficha de plantilla, registro de capacitaciones y base de datos).
– Los empleados de la empresa deben usar cuentas de usuario individuales y contraseñas únicas.
– La empresa debe contar con reglas de contraseñas, y los empleados deben usar contraseñas sólidas.
– El acceso de usuarios a la ciberseguridad/TI debe estar restringido y basarse en la descripción del puesto del empleado o de sus tareas asignadas.
– El acceso del usuario autorizado debe ser revisado por la empresa con regularidad para garantizar que el acceso a sistemas confidenciales se base en los requisitos del puesto del usuario.
– El sistema de ciberseguridad/TI y las estaciones de trabajo informáticas deben estar protegidos por antivirus y firewall. Estas aplicaciones deben recibir actualizaciones de seguridad periódicas.
– Si se produce una violación de datos o un evento ocasiona la pérdida de datos o equipos, los procedimientos de ciberseguridad/seguridad de TI de la empresa deben incluir la recuperación o sustitución de sistemas de TI o de datos.
– La empresa debe implementar un sistema para identificar el acceso no autorizado a sistemas de TI o de datos de la empresa.
– La empresa debe implementar un sistema para identificar el abuso de políticas y procedimientos de TI, incluidos el acceso incorrecto a sistemas internos o sitios web externos y la manipulación o alteración de datos comerciales por parte de empleados o contratistas.
– La empresa debe contar con medidas disciplinarias por escrito (SOP) para infractores de las políticas y procedimientos de TI de la empresa.
– La seguridad de la infraestructura de TI de la empresa se debe probar con regularidad.
– Las políticas y procedimientos de ciberseguridad/TI de la empresa se deben aplicar a empleados que tienen permitido usar dispositivos personales para realizar el trabajo de la empresa.
– Las políticas y procedimientos de ciberseguridad/TI de la empresa se deben aplicar a usuarios que tienen permitido conectarse a la red de manera remota.
– La empresa debe usar tecnologías seguras, como redes privadas virtuales (*virtual private networks*, VPN) para permitir a los empleados el acceso a la Intranet de la empresa de manera segura cuando se encuentren fuera de la oficina.
– Los procedimientos de ciberseguridad/seguridad de TI se deben designar para prevenir el acceso remoto de usuarios no autorizados.

* La documentación que detalla/demuestra los procedimientos de ciberseguridad de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

- **Seguridad de transporte: Seguridad de Transmisión e Instrumentos de Tráfico Internacional (IIT)**

Esté preparado para analizar de qué manera la empresa procesa el cargamento y los envíos, incluidos los procedimientos de seguridad para el almacenamiento del cargamento listo para enviar, procedimientos de carga, la inspección de instrumentos de tráfico internacional (*instruments of international traffic*, IIT), como contenedores *o* acoplados, protocolos de sellado y el seguimiento y monitoreo del envío.

* Si la empresa no maneja de manera física el cargamento o los envíos (p. ej., agentes de aduanas)
o
* Si la empresa terceriza o contrata elementos de transmisión y seguridad de los IIT
o
* Si la empresa no es responsable de llevar a cabo ningún elemento de transmisión y seguridad de los IIT

– Esté preparado para analizar de qué manera la empresa garantiza la implementación de procedimientos que cumplen con los MSC de la CTPAT.

(Según corresponda): el equipo de validación de la CTPAT revisará la forma en que se protege el cargamento en el punto de origen (antes de la carga), el proceso de carga, la forma en que se inspeccionan los IIT antes de la carga (p. ej., inspecciones de 7-8 o 17 puntos), cómo se sellan los IIT cargados, cómo se almacenan los IIT y cómo la empresa sigue y monitorea los IIT cargados desde la fábrica (o el punto de carga) hasta el puerto/terminal.

(Según corresponda)
– Los IIT (p. ej., contenedores de envío, acoplados y camiones furgones) se deben inspeccionar antes de la carga.
– La empresa debe contar con un SOP por escrito para inspecciones de seguridad de los IIT.
– La empresa debe documentar las inspecciones de los IIT (p. ej., lista de verificación de inspección).
– Los sellos utilizados para proteger los IIT deben cumplir con la norma ISO 17712.
– Se debe controlar el inventario de sellos y se deben implementar protocolos de sellos.
  * Se entiende que los envíos aéreos a los EE. UU. pueden no utilizar contenedores o sellos *
– La empresa debe contar con un SOP por escrito para protocolos de sellos.
– Las transmisiones y los IIT se deben almacenar en un área segura para evitar el acceso no autorizado.
– La empresa debe contar con un SOP por escrito para el almacenamiento de los IIT.
– La empresa debe trabajar con proveedores de servicios de logística y transporte para realizar un seguimiento de las transmisiones y envíos del origen al puerto/terminal o al punto de destino final.
– La empresa debe contar con un SOP por escrito para seguimiento y monitoreo.

* La documentación que detalla/demuestra los procedimientos de transmisión y seguridad de los IIT debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad de procedimientos: Informes y protocolos de notificaciones**

Esté preparado para analizar los procedimientos de la empresa para informar incidentes de seguridad y actividades sospechosas.

– La empresa debe contar con un SOP por escrito para instrucciones/protocolos de informes (p. ej., para una violación de la seguridad de envíos).
– El SOP por escrito de la empresa para instrucciones/protocolos de informes debe incluir una lista de información de contacto para notificaciones.

– Se debe capacitar a los empleados de la empresa con respecto a las instrucciones/protocolos de informes.
– Después de un importante incidente de seguridad, la empresa debe iniciar un análisis posterior al incidente (*post-incident analysis*, PIA).
– Los hallazgos del PIA de la empresa se deben documentar y deben estar disponibles para el SCSS.
– Los procedimientos de la empresa para instrucciones/protocolos de informes se deben divulgar a socios comerciales clave.
* La documentación que detalla/demuestra los procedimientos de informes y notificaciones de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad de procedimientos: Procesamiento de envíos, documentación**

Esté preparado para analizar la función de la empresa en el procesamiento (o la agilización) de un envío típico, lo que incluye cómo comienza el proceso de envío, cómo se reciben los datos de envío, cómo se verifican dichos datos, cómo se cotejan los documentos de envío para garantizar la precisión y cómo se presentan los datos de envío a Aduanas y Protección de Fronteras (Customs and Border Protection, CBP) de los EE. UU.

* Debe contar con un paquete de documentación de envío para que el equipo de validación de la CTPAT lo revise, para incluir todos los documentos de envío conservados que están relacionados con el procesamiento del envío (p. ej., orden de compra, factura, lista de contenido, conocimiento de embarque [*bill of lading*, BOL], despacho aduanero, orden de entrega, etc.) *

* El paquete de documentos debe incluir documentos de un envío reciente importado en los EE. UU., según corresponda, y se prefiere que el paquete sea específico de la cadena de suministro que se está revisando para la validación actual *

– La empresa debe contar con un SOP por escrito para procesar (o facilitar) un envío típico.
– La empresa debe garantizar que se hayan implementado los protocolos de la documentación de envío en el origen.
– Se debe capacitar a la empresa y a los empleados relevantes para revisar documentos de envío e identificar anomalías o envíos sospechosos.
* La documentación que detalla/demuestra los procedimientos de procesamiento de envíos de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad de procedimientos: Procesamiento de envíos, recepción de cargamento y envíos**

(Según corresponda): esté preparado para analizar la función de la empresa de recibir cargamento y envíos, lo que incluye la forma en que los controladores se identifican de manera positiva, cómo se verifican los números de contenedores y sellos antes de la descarga, de qué manera se reconcilia el cargamento durante el proceso de descarga y cómo se identifican, investigan, resuelven e informan las discrepancias y anomalías (según corresponda).

* Si la empresa no maneja de manera física el cargamento o los envíos (p. ej., agentes de aduanas)
o
* Si la empresa terceriza o contrata elementos de recepción de cargamento y envíos
o
* Si la empresa no es responsable de llevar a cabo ningún elemento de recepción de cargamento y envío
– Esté preparado para analizar de qué manera la empresa garantiza la implementación de procedimientos que cumplen con los MSC de la CTPAT.
(Según corresponda):

– La empresa debe contar con un SOP por escrito para la recepción de cargamentos y envíos.
– La empresa debe contar con un SOP por escrito para abordar discrepancias y anomalías.
– La empresa debe contar con un SOP por escrito para instrucciones/protocolos de informes (p. ej., para una violación de la seguridad de envíos).
– Los procedimientos de la empresa para instrucciones/protocolos de informes se deben divulgar a socios comerciales clave.
* La documentación que detalla/demuestra los procedimientos de recepción de cargamento y envío de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad de transporte: Seguridad agrícola**

– La empresa debe contar con un SOP por escrito para inspecciones agrícolas de los IIT.
* La documentación que detalla/demuestra los procedimientos de seguridad agrícola de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad física y de las personas: Seguridad física**

Esté preparado para analizar y demostrar la seguridad de la instalación de la empresa.

– La instalación debe contar con barreras físicas o disuasiones que eviten el acceso no autorizado.
– La instalación debe contar con iluminación adecuada tanto en su interior como en el exterior.
– La empresa debe contar con un SOP por escrito para la seguridad de la instalación.
– La empresa debe contar con un SOP por escrito para las inspecciones de la instalación.
– La empresa debe documentar las inspecciones de la instalación (p. ej., lista de verificación de inspección).
(Según corresponda):

* Si la instalación cuenta con puertas para el ingreso o la salida de vehículos o personal

– Las puertas de la instalación deben contar con personal o estar monitoreadas.

(Según corresponda):

* Si la instalación está monitoreada por un sistema de alarma contra intrusiones
o
* Si la instalación está monitoreada por un sistema de cámaras de videovigilancia

– La alarma o las cámaras de la instalación deben estar protegidas de manera física contra el acceso no autorizado.
– La empresa debe contar con un SOP por escrito que rija el uso no autorizado, el mantenimiento (inspecciones de operación adecuada) y la protección de la tecnología de seguridad (alarma y cámaras).

– El SOP de tecnología de seguridad por escrito de la empresa se debe revisar y actualizar una vez al año.
– Las cámaras de la empresa se deben posicionar para abarcar áreas clave de la instalación que pertenezcan al proceso de envío.
– El personal designado de la empresa (p. ej., gestión, seguridad) debe llevar a cabo revisiones aleatorias de filmaciones de las cámaras para verificar si los procedimientos de seguridad del cargamento se están siguiendo adecuadamente de conformidad con la ley.
* La documentación que detalla/demuestra los procedimientos de seguridad de la instalación de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad física y de las personas: Controles de acceso físico**

Esté preparado para analizar y demostrar los controles de acceso físico a la instalación, incluido lo siguiente:

– Cómo la empresa controla el movimiento de empleados y visitantes durante toda la instalación.
– Cómo la empresa identifica de manera positiva a empleados y visitantes.
– Cómo la empresa controla el acceso de los empleados a áreas restrictas.
– El proceso utilizado para aceptar visitantes, proveedores de servicio y controladores.
– La empresa debe contar con un SOP por escrito para la emisión/activación y recuperación/desactivación de dispositivos de acceso (p. ej., credenciales de identificación [id.], tarjetas de identificación de frecuencia de radio [*radio frequency identification*, RFID], claves de copia impresa, códigos de alarma y acceso informático [TI]).
– La empresa debe contar con un SOP por escrito para instrucciones/protocolos de informes (p. ej., personas no autorizadas).

(Según corresponda): se debe contar con ejemplos de los siguientes ítems para revisión, incluidos los siguientes:

– Credencial de id. del empleado
– Tarjeta de RFID del empleado
– Formulario de bienes de la empresa o lista de verificación de salida
– Credencial de id. del visitante
– Registro del visitante, registro del conductor, registro de depósito o recepción del envío
– Instrucciones de trabajo (SOP) para guardias de seguridad

* La documentación que detalla/demuestra los procedimientos de control de acceso físico de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad física y de las personas: Seguridad del personal**

Esté preparado para analizar de qué manera la empresa evalúa a los posibles empleados y verifica periódicamente a los actuales.

– La empresa debe contar con un SOP por escrito para seleccionar a los empleados.
– La empresa debe verificar los datos de los empleados (p. ej., información de solicitud, historial de empleo, referencias).
– La empresa debe utilizar una lista de verificación de datos del empleado o algo similar.
– La empresa debe conservar datos de los empleados y la información de selección en archivos individuales.
– La empresa debe realizar evaluaciones de antecedentes de empleados y nuevas investigaciones periódicas.
– La empresa debe contar con un SOP por escrito relacionado con el código de conducta del empleado.
– La empresa debe contar con un SOP por escrito para rescindir el vínculo con el empleado.

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

* Debe contar con un archivo de empleado de muestra disponible para la revisión *

* La documentación que detalla/demuestra los procedimientos de seguridad del personal de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

- **Seguridad física y de las personas: Educación, capacitación y concientización**

Esté preparado para analizar el programa de educación, capacitación y concientización de la empresa.

– La empresa debe implementar un programa de capacitación en seguridad y concientización sobre amenazas para los empleados.
– Se debe capacitar a los empleados de la empresa para informar incidentes de seguridad y actividades sospechosas.
– La empresa debe ofrecer a los empleados un método de informes anónimos (p. ej., casilla de sugerencias o línea telefónica directa).
– La empresa debe capacitar a los empleados relevantes para revisar documentos de envío, identificar anomalías e identificar envíos sospechosos.
– La empresa debe capacitar a los empleados relevantes para identificar los indicadores de advertencia de lavado de dinero basado en el comercio y financiación del terrorismo.
– La capacitación en seguridad y el programa de concientización deben incluir todos los requisitos de seguridad de la CTPAT.
– La empresa debe contar con capacitación especializada para puestos delicados.
– La empresa debe realizar capacitación periódica de perfeccionamiento.
– La empresa debe documentar la capacitación recibida por los empleados (p. ej., ficha de plantilla, registro de capacitaciones y base de datos).
– La empresa debe contar con un SOP por escrito para el programa de educación, capacitación y concientización sobre seguridad (p. ej., capacitador, público, agenda, frecuencia y materiales de capacitación).

(Según corresponda):

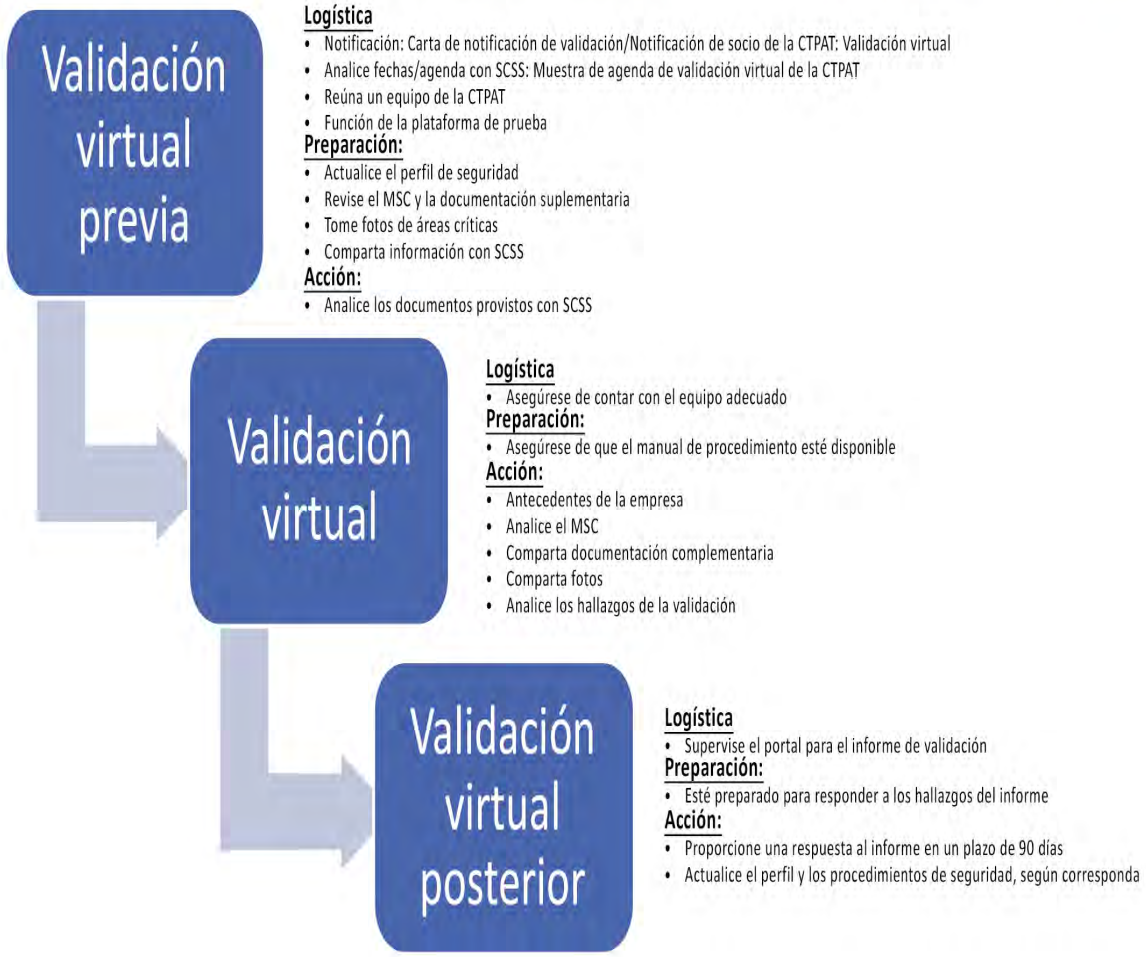
– La empresa debe capacitar a los empleados relevantes con respecto a las políticas y procedimientos de ciberseguridad/TI.
– Los empleados de la empresa que gestionan los sistemas de tecnología de seguridad de TI deben recibir capacitación.
– La empresa debe capacitar a los empleados relevantes para realizar inspecciones agrícolas y de seguridad de transmisiones vacías e IIT (p. ej., contenedores, acoplados).
– La capacitación de transmisión e inspección de los IIT de la empresa debe incluir los siguientes temas: ocultación de contrabando en compartimentos ocultos (y compartimentos naturales), señales de contaminación por pestes y cumplimiento de materiales de embalaje de madera (*wood packaging material*, WPM).

* La documentación que detalla/demuestra los procedimientos de concientización sobre educación, capacitación y seguridad de la empresa debe estar disponible para su revisión por parte del equipo de validación de la CTPAT durante la reunión *

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

Guía de validación virtual



Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

CARTA DE INVITACIÓN DE MUESTRA A LA VALIDACIÓN VIRTUAL DE LA CTPAT

1300 Pennsylvania Ave. NW,
Rm. 2.2A
Washington, DC 20229

U.S. Customs and Border Protection

Fecha
Nombre de POC
Título de POC
Nombre de la empresa
Dirección

Estimado/a Sr./Sra. (Nombre de POC):

Como socio confiable de la CTPAT con un historial demostrado de cumplimiento de los criterios de seguridad mínima del programa y las leyes y disposiciones de CBP, se seleccionó a Nombre de la Empresa para llevar a cabo una validación virtual. Este enfoque innovador sobre el proceso de validación pretende desarrollar nuestra sociedad existente y los beneficios actuales, reducir los costos del sector público-privado asociados con la visita en el sitio y aprovechar la tecnología disponible para ofrecer una alternativa a métodos tradicionales de verificación de la cadena de suministro que tenga adaptabilidad en diferentes sectores y rutas comerciales.

¿Qué es una validación virtual?

La validación virtual incluirá una estrecha colaboración entre el socio de la CTPAT y el especialista de Seguridad de la Cadena de Suministro (SCSS) en el uso de tecnología disponible para realizar reuniones virtuales y verificaciones nacionales y extranjeras de la cadena de suministro, según corresponda, determinar el cumplimiento de los criterios de seguridad mínima de la CTPAT e identificar y abordar el riesgo dentro de la cadena de suministro. El proceso de validación virtual utilizará las aplicaciones de conferencia web y videoconferencia para conectar de manera segura a la empresa y a sus correspondientes instalaciones de la cadena de suministro con el SCSS, y para permitir un intercambio, una revisión y una validación seguros de datos de seguridad pertinentes de la cadena de suministro en un entorno en tiempo real.

Qué esperar a continuación

Su SCSS se pondrá en contacto con usted en breve para abordar el alcance del proceso de validación virtual, que incluirá la confirmación de la capacidad de la empresa de realizar y utilizar este beneficio, como también una solicitud de cualquier información adicional que pueda ser necesaria. Una vez completada la revisión del documento y acordada la fecha y hora de la validación virtual, el SCSS invitará a la empresa y a sus participantes seleccionados a iniciar el proceso de validación virtual.

Validación virtual

En la medida de lo posible, la validación virtual reflejará el proceso de validación física e incluirá una revisión de la documentación escrita, los procedimientos y las medidas de seguridad implementadas para garantizar la cadena de suministro internacional del socio de la CTPAT. En función de las capacidades técnicas disponibles, se puede llevar a cabo una revisión más inmersiva de requisitos críticos de los criterios de seguridad mínima para incluir la seguridad física de la instalación mediante la aplicación de videoconferencias y conferencias web.

Agenda y guía de muestra de la validación virtual

Última actualización: 18 de octubre de 2021

Seguimiento e informe de validación virtual

Después de completar la validación virtual, el socio de la CTPAT y el SCSS analizarán los hallazgos, evaluarán la efectividad de las medidas de seguridad de los socios y señalarán los puntos débiles y las deficiencias que deben abordarse. Los hallazgos de la validación virtual se documentarán en el informe de validación y se reenviarán al socio de la CTPAT para su revisión; incluirán recomendaciones identificadas de la cadena de suministro o prácticas recomendadas.

Le agradecemos por su respaldo continuo y su cumplimiento demostrado de los criterios de seguridad mínima del programa de la CTPAT, y esperamos poder colaborar con usted en este emprendimiento para adaptarnos a los desafíos presentados por la economía global dinámica y el aumento de la amenaza de terrorismo y contrabando.

Atentamente.

Manuel A. Garza, Jr.
Director, CTPAT
Oficina de Operaciones de Campo
Aduanas y Protección de Fronteras de los EE. UU.

Programa de la CTPAT

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229