BASC

BUSINESS ALLIANCE FOR SECURE COMMERCE

CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM

Críterios Mínimos de Seguridad

Carlos E. Ochoa

Branch Chief
Trade Engagement and Communications
Washington, D.C.

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
VIGILANCE INTEGRITY SERVICE

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Criterios de Seguridad – Actualización

Actualización de los criterios: Proceso duró más de 3 años.
Primera vez que los criterios del programa son actualizados.
Trabajo hecho en colaboración con el sector privado.
Consideramos las pequenas y medianas empresas

- Principio del 2016 – Equipo de trabajo (50 personas) creado bajo el marco del COAC.
- Equipo de Trabajo – Seis Grupos / Cada grupo un tema en particular
- Teleconferencias, Webinars, Reuniones en persona en Washington: Llegar a un consenso.
- Mayo 2019 – Criterios publicados a través del Portal de CTPAT.
- Enero 2020 – Inicio de validaciones basadas en nuevos criterios

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE · SERVICE · INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Criterios de Seguridad – Actualización

- Leyes Federales / SAFE Port Act 2006 y TFTF Act de 2015
- Reflejar la Misión de CBP / 2003 – Nueva Agencia
- Cambios que Afectaron el Comercio / Rol de la Tecnología
- Reflejar la Experiencia / CTPAT, OMA / Otros Pogramas OEA
- Terrorismo y Actividades Criminales
  - ✓ Ataques cibernéticos
  - ✓ Lavado de dinero

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE SERVICE INTEGRITY

Críterios – Organización y Estructura

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

AREAS DE ENFOQUE	NUMERO DE CATEGORIA DE SEGURIDAD	CATEGORIAS DE SEGURIDAD
I. Seguridad Corporativa	1	Visión de Seguridad y Responsabilidad
	2	Análisis de Riesgo
	3	Requisitos de Socios de Negocio
	4	Seguridad Cibernetica
II. Seguridad en la Transportación	5	Seguridad de Transporte Y IIT
	6	Seguridad de Sellos
	7	Seguridad de Procedimientos
	8	Seguridad Agrícola
III. Seguridad Física y deL Personal	9	Controles de Acceso Físico
	10	Seguridad Física
	11	Seguridad del Personal
	12	Capacitación en Seguridad, Amenazas y Concientización

Nueva Estructura

3 Areas de Enfoque

12 Críterios de Seguridad

ID Números

Guía de Implementación

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Categoría Nueva: Seguridad debe de ser una parte integral de la cultura de una compañía / Incorporada en todos sus procesos.

Sección 1 – 4 Criterios – Aplican a todos los Miembros del programa (CORE).

Cultura organizacional y filosofía de gestión que:

- Promueve una cultura que fomenta y exige un compromiso de cumplimiento de la ley.
- Promueve la seguridad como un objetivo y responsabilidad de toda la empresa.
- Describe las responsabilidades de cumplimiento, detalla los controles internos, las prácticas de auditoría, las políticas de documentación y los procedimientos disciplinarios.
- Reconoce la importancia del papel que desempeña el Punto de Contacto de la compañía o empresa con CTPAT.

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE SERVICE INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

1.1 – Promover la Seguridad - Deberían

- Para fomentar una cultura de seguridad, los miembros de CTPAT deberían demostrar su compromiso con la seguridad de la cadena de suministro y el programa CTPAT mediante una declaración de apoyo.

- La declaración debería estar firmada por un alto funcionario de la empresa y exhibirse en lugares adecuados de la empresa.

REX CARGO
a Rex America Company

Security·Policy:¶

Rex·Cargo·is·committed·to·protecting·the·interests·of·our·customers,·partners·and·suppliers,·ensuring·that·all·goods·and·related·documents,·will·be·protected·from·alterations,·damage·or·loss,·preventing·pollution·by·terrorism·or·drug·trafficking,·through·the·establishment·and·continuous·improvement·of·the·management·system·in·control·and·security.·Ensuring·clean,·secure·and·punctual·cargo.¶

Se Crea Seguridad al Promoverla Internamente / Externamente

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE · SERVICE · INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Rol proactivo de la gerencia acentuado a lo largo de los críterios

- Evaluación de riesgos: gestión de crisis / planes de recuperación / reanudación empresarial.
- Socios comerciales: Firma del gerente en cuestionarios de seguridad.
- Transporte / IIT: La gerencia realiza inspecciones aleatorias de medios de transporte; auditorías aleatorias de procedimientos de seguimiento y monitoreo.
- Sello: Gestión de auditorías de sellos.
- Procedimiento: exámenes aleatorios de las pertenencias del conductor.
- Físico: revisión periódica y aleatoria del metraje (footage) de la cámara de seguridad.

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE SERVICE INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Caso Estudio – Confiscaciones de Narcóticos en Aerolíneas - 2014

Factores Contribuyentes:

- Falta de supervisión a procedimientos de seguridad
- Complacencia
- No siguieron procesos de seguridad establecidos por la empresa
- No monitoreaban los equipos y bienes de la compañía

Resultado:

- Red de conspiración interna y externa profundamente arraigada que involucró a equipos de limpieza, empresas de catering, mecánicos, manipuladores de equipaje y personal de seguridad.

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE · SERVICE · INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

1.3 – Componente de Revisión Escrita - Debe

- El programa de seguridad - Diseñar, respaldar e implementar a través de un adecuado componente de revisión por escrito.

- Propósito de este componente de revisión: documentar que se cuenta con un sistema en vigor mediante el cual el personal rendirá cuentas respecto a sus responsabilidades y que todos los procedimientos de seguridad descritos por el programa de seguridad se están implantando según lo diseñado.

- El plan de revisión debe actualizarse según sea necesario en función de los cambios pertinentes en las operaciones y el nivel de riesgo de una organización.

Documentados ➡ Responsabilidad / Transparencia

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
VIGILANCE SERVICE INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

1.4 – Punto de Contacto de La Empresa con CTPAT - Debe

- El punto de contacto (POC) de la empresa con CTPAT debe conocer los requisitos del programa.

- Estas personas deben proporcionar actualizaciones periódicas a la alta gerencia con respecto a asuntos relacionados con el programa, entre ellos el avance o los resultados de cualquier auditoría, ejercicios relacionados con la seguridad y las validaciones de CTPAT.

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
VIGILANCE SERVICE INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Importancia del Punto de Contacto de la Compañía con CTPAT

Año Fiscal 2013 - 114 Miembros Eliminados del Programa

- No respondieron al reporte de validación - 53 (46.5% del total)
- No completaron su auto-evaluación anula (self-assessment) o actualizaron su perfil de seguridad - 31 (27.2% del total)
- No mantuvieron el compromise con el programa (e.g., to trabajaron con el Especialista de CTPAT para coordinar la fecha de la validación) - 2
- Incidente de Seguridad – 7

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
VIGILANCE SERVICE INTEGRITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

3.9 – Programa de Cumplimiento Social - Deberían

Si es un importador, exportador o fabricantes, tener un **programa de responsabilidad social documentado** que, como mínimo, aborde cómo la empresa garantiza que los bienes que se importan o se exportan no se extrajeron, produjeron o fabricaron, de manera total o parcial, con formas de trabajo prohibidas (trabajo forzado, trabajo encarcelado, o trabajo con menores).

Guida de Implementación - Un programa de cumplimiento social se refiere a una serie de políticas y prácticas mediante las cuales una empresa busca garantizar el máximo cumplimiento de los aspectos de su código de conducta que cubren asuntos sociales y laborales.

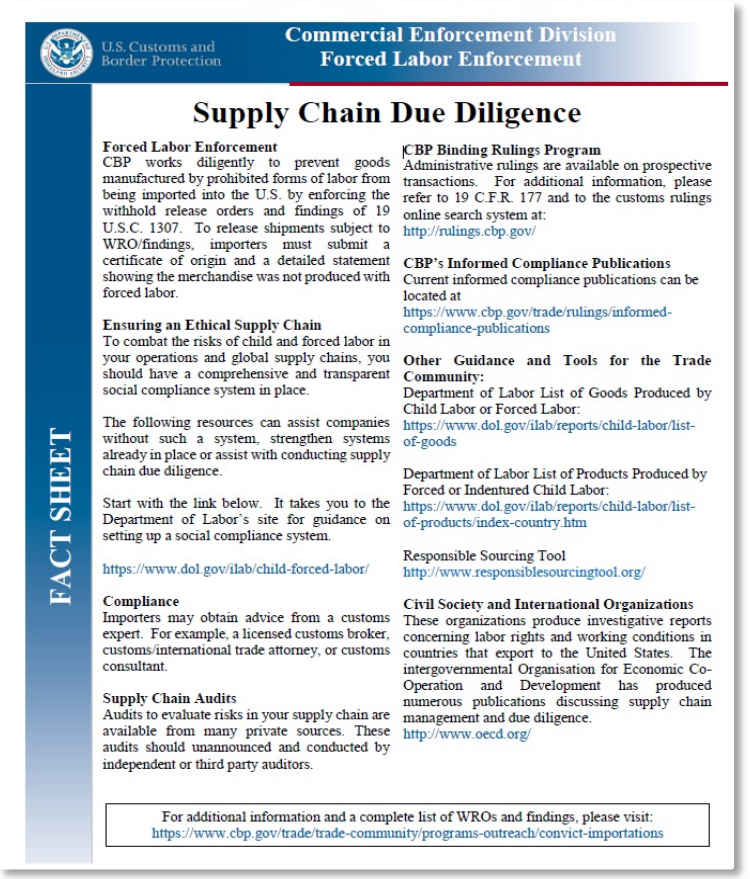
U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE · SERVICE · INTEGRITY

Bases Legales

- Convenciones de la Organización Internacional del Trabajo : No. 29 – 1930 y No. 105 - 1957
- Tariff Act of 1930
- The Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA) – Section 909
- Federal Acquisition Requirements (FAR) – clause 52.222-50
- Countering America's Adversaries Through Sanction Act (CAATSA) – Cubre sanciones contra Rusia, Iran y Corea del Norte.
- California Transparency Act
- United Kingdom Modern Slavery Act
- Francia – Corporate Duty of Vigilance Law.

Críterio 3.9 - Trabajo Forzoso

- Applica a importadores, exportadores, y manufactureros
- **El trabajo forzoso presenta un riesgo triple para las empresas**, independientemente de la industria o el tamaño de la empresa: riesgo de continuidad del negocio, riesgo de marca o reputación y riesgo legal
- Si el riesgo se materializa:
  - ✓ Reacción negativa de los consumidores
  - ✓ Pérdida de relaciones comerciales
  - ✓ Retrasos en la producción
  - ✓ Órdenes de detención de CBP (retener órdenes de liberación)
- Hay un vínculo directo entre el trabajo forzoso y otros problemas que afectan al seguridad de la cadena de suministro



U.S. Customs and Border Protection

Commercial Enforcement Division
Forced Labor Enforcement

FACT SHEET

Supply Chain Due Diligence

Forced Labor Enforcement
CBP works diligently to prevent goods manufactured by prohibited forms of labor from being imported into the U.S. by enforcing the withhold release orders and findings of 19 U.S.C. 1307. To release shipments subject to WRO/findings, importers must submit a certificate of origin and a detailed statement showing the merchandise was not produced with forced labor.

Ensuring an Ethical Supply Chain
To combat the risks of child and forced labor in your operations and global supply chains, you should have a comprehensive and transparent social compliance system in place.

The following resources can assist companies without such a system, strengthen systems already in place or assist with conducting supply chain due diligence.

Start with the link below. It takes you to the Department of Labor's site for guidance on setting up a social compliance system.

https://www.dol.gov/ilab/child-forced-labor/

Compliance
Importers may obtain advice from a customs expert. For example, a licensed customs broker, customs/international trade attorney, or customs consultant.

Supply Chain Audits
Audits to evaluate risks in your supply chain are available from many private sources. These audits should unannounced and conducted by independent or third party auditors.

CBP Binding Rulings Program
Administrative rulings are available on prospective transactions. For additional information, please refer to 19 C.F.R. 177 and to the customs rulings online search system at:
http://rulings.cbp.gov/

CBP's Informed Compliance Publications
Current informed compliance publications can be located at
https://www.cbp.gov/trade/rulings/informed-compliance-publications

Other Guidance and Tools for the Trade Community:
Department of Labor List of Goods Produced by Child Labor or Forced Labor:
https://www.dol.gov/ilab/reports/child-labor/list-of-goods

Department of Labor List of Products Produced by Forced or Indentured Child Labor:
https://www.dol.gov/ilab/reports/child-labor/list-of-products/index-country.htm

Responsible Sourcing Tool
http://www.responsiblesourcingtool.org/

Civil Society and International Organizations
These organizations produce investigative reports concerning labor rights and working conditions in countries that export to the United States. The intergovernmental Organisation for Economic Co-Operation and Development has produced numerous publications discussing supply chain management and due diligence.
http://www.oecd.org/

For additional information and a complete list of WROs and findings, please visit:
https://www.cbp.gov/trade/trade-community/programs-outreach/convict-importations

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

How does cybersecurity impact trade?

Working directly with its trade partners, CBP facilitates approximately **$2.4 trillion** in trade revenue each year.

Weak cybersecurity can have significant implications for trading partners

$445B
Estimated losses to the global economy in 2013 due to cyber crimes, including both the gains to criminals and the cost of recovery and defense

456
Hours to restore one vessel's seaworthiness due to malware

90%
Percentage of world's goods on 400,000 ships left potentially vulnerable to GPS spoofing, jamming, or interception

Cyber threats will only continue to increase.

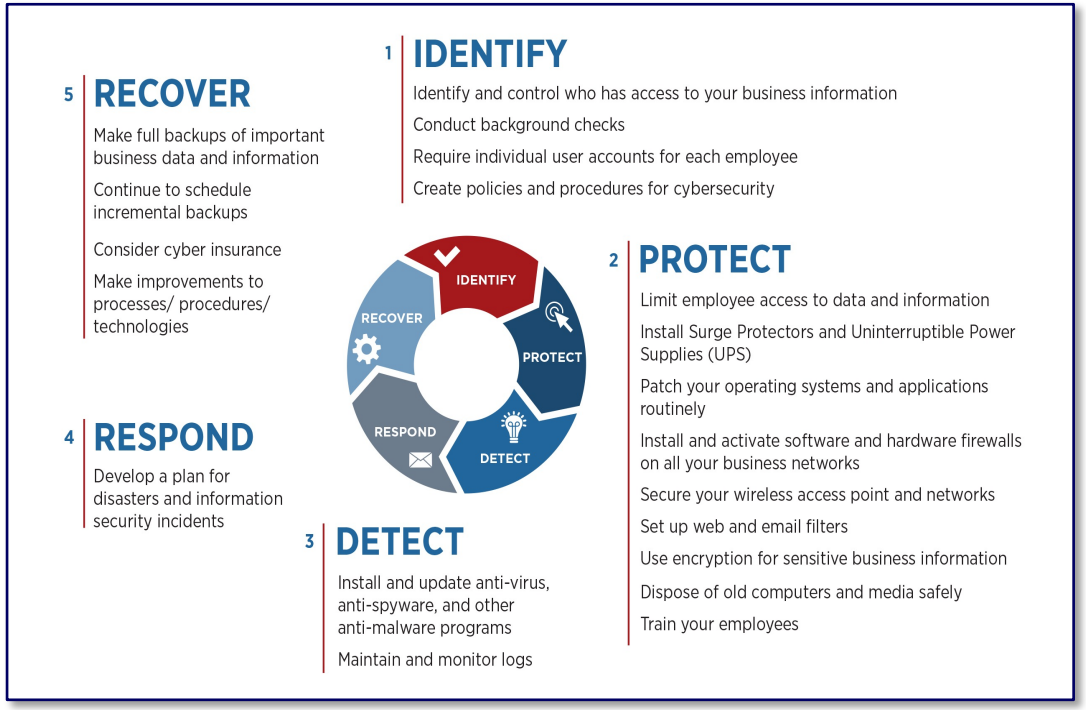
"In 2013, 'cyber' bumped 'terrorism' out of the top spot on our list of national threats… **And cyber has led our report every year since.**"
– James Clapper, Director of National Intelligence
January 29, 2016

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Ciberseguridad – Clave para salvaguardar los activos más preciados de una empresa: propiedad intelectual, información de clientes, datos financieros y comerciales y registros de empleados.

- Categoría de 13 Requisitos
- Aplican a todos los Miembros del Pograma y Sus Socios de Negocio
- Basados en Estándares de la Industria
- Pequeñas y Medianas Empresas Fueron Tomadas en Cuenta



U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY

Criterio 4.2 - Uso de Software/Hardware para Proteger Sistemas Informáticos – Deben

- Software para protegerse contra el malware
- Se requiere el uso de un programa de software de protección antivirus en cada estación de trabajo
- Cortafuegos: protegen la computadora de ataques externos o tráfico de red innecesario.
- Procedimientos para prevenir ataques de ingeniería social (incluye capacitación a los usuarios).

91% de los ciberataques comienzan con un correo electrónico. FireEye

Críterio 4.3 – Probar la Seguridad de sus Sistemas de Red - Deben

- Pruebe sus protocolos de seguridad para asegurarse de que realmente están trabajando para identificar nuevas vulnerabilidades.

- Realice análisis (scans) de vulnerabilidades para detectar vulnerabilidades.

Críterio 4.4 – Compartir Información Sobre Amenazas – Deberían

- Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC) - Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerta CTPAT – Ciberseguridad

Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

Key Federal Points of Contact

Threat Response	*Asset Response*
Federal Bureau of Investigation (FBI) **FBI Field Office Cyber Task Forces:** http://www.fbi.gov/contact-us/field **Internet Crime Complaint Center (IC3):** http://www.ic3.gov *Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.* *Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.*	**National Cybersecurity and Communications Integration Center (NCCIC)** **NCCIC:** (888) 282-0870 or NCCIC@hq.dhs.gov **United States Computer Emergency Readiness Team:** http://www.us-cert.gov *Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.*
National Cyber Investigative Joint Task Force **NCIJTF CyWatch 24/7 Command Center:** (855) 292-3937 or cywatch@ic.fbi.gov *Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.*	CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK **U.S. Customs and Border Protection** **CTPAT Program - Supply Chain Security Specialist** **Phone Number:** **E-Mail:** _____@cbp.dhs.gov ***Minimum Security Criterion - 4.4 - Cyber security policies should address how a Member shares information on cyber security threats with the government and other business partners.***
United States Secret Service **Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):** http://www.secretservice.gov/contact/field-offices *Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information*	**Other Related CTPAT Requirements:** ***Minimum Security Criterion - 7.23 - CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process.***

Críterio 4.8 – Cuentas Individuals / Uso de Contraseñas o Frases Secretas – Deben

- Requisito que ya existía - con varios cambios.
- Autenticación – 2FA o MFA preferido
- Preferimos el uso de largas frases secretas a contraseñas
- Requiere el cambio de contraseñas tan pronto sea posible si existen indicios o sospecha razonable de que han sido comprometidas – ya no cada 90 días.

Críterio 4.9 – Uso de Redes Privadas Virtuales (VPN) – Deben

- Objetivo - tener procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados.

Críterio 4.10 – Dispositivos Personales Deben de Cumplir con Polícas de Seguridad de la Empressa – Deben

- Los dispositivos personales incluyen medios de almacenamiento como discos compactos (CD), reproductores de video (DVD) y unidades de memoria USB. Se debe tener cuidado si se permite a los empleados conectar sus dispositivos personales a sistemas individuales, ya que estos dispositivos de almacenamiento de datos pueden estar infectados con programas malignos que podrían propagarse a través de la red de la empresa.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

8.1 – Procedimientos Para Prevenir la Contaminación Agrícola – Deben

Los miembros de CTPAT deben, de acuerdo con su modelo comercial, tener procedimientos por escrito diseñados para evitar la contaminación de plagas visibles en conformidad con las reglamentaciones de los Materiales de Embalaje de Madera (WPM).

Hasta el 40 por ciento de la producción agrícola mundial se pierde debido a plagas que afectan diferentes cultivos.

Organización de las Naciones Unidas para la Agricultura y la Alimentación (FAO).

Las medidas visibles de prevención de plagas se deben cumplir en toda la cadena de suministro. Las medidas relacionadas con las reglamentaciones WPM deben cumplir con las Normas Internacionales para Medidas Fitosanitarias N.º 15 (NIMF 15) de la Convención Internacional de Protección Fitosanitaria (CIPF).

U.S. CUSTOMS AND BORDER PROTECTION · DEPARTMENT OF HOMELAND SECURITY · VIGILANCE · SERVICE · INTEGRITY

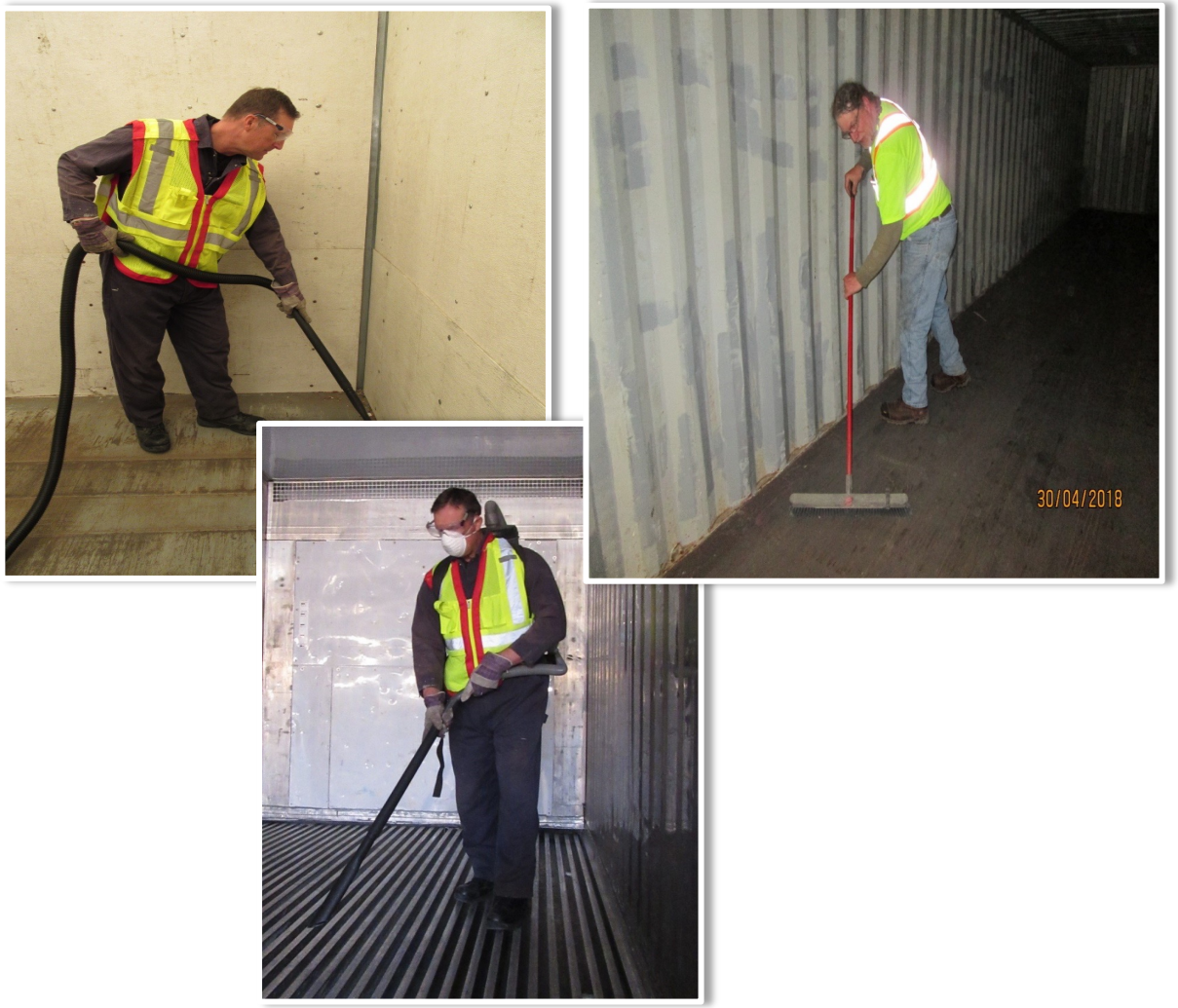
Eliminación de Plagas y Contaminantes = Facilitación

- Categoría de un Solo Requisito – Aplica a todos los miembros de la cadena.
- Basado en Normas Internacionales
- No es algo nuevo que las empresas tengan que hacer.
- Solo plagas y contaminantes "visibles" según la definición de la OMI. No se necesita equipo especializado ni costoso.
- Material de embalaje de madera: enfoque en WPM porque WPM es uno de los métodos más comunes para la contaminación por plagas.
- Beneficios Se hacen Realidad

Seguridad Agrícola

Insects & Snails	Plant Material & Seeds	Garbage & Organic Material
 Snails	 Cogon Grass	 Manure
 Grasshoppers	 Spilled seed on trailer floor	 Animal Blood
 Asian Gypsy moth egg masses	 Weed seeds stuck to WPM	 Soil Contamination
 Khapra Beetle Larvae	 Cottonseed in rail car springs	 Garbage contamination on rail

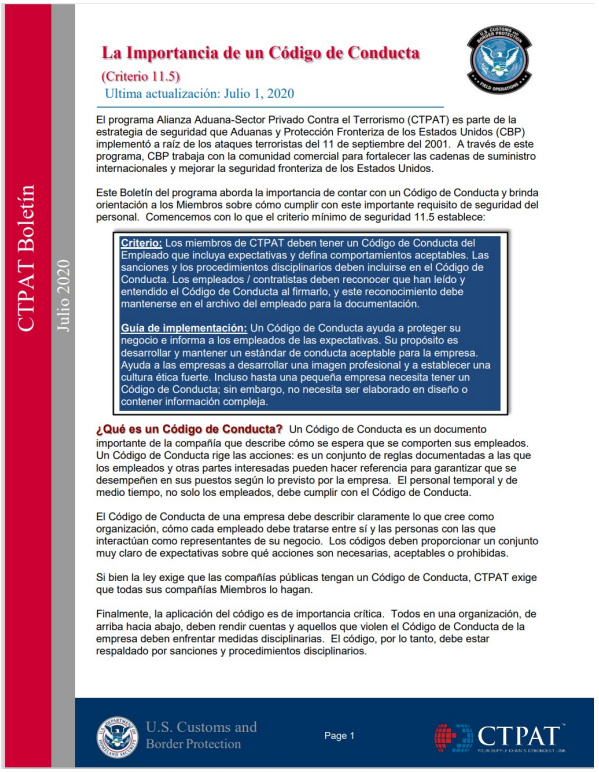
Protección de la cadena de suministro de plagas y contaminantes visibles – Herramientas



Codigo de Conducta – Deben

Miembros de CTPAT deben de tener un Código de conducta. El cual define expectativas y conductas aceptables.

- ✓Permite a la Alta gerencia establecer el marco necesario en cuanto a la conducta corporativa y de su personal, basado en principios y valores.
- ✓Ayuda a los empleados a visualizar los principios y valores de la empresa, los cuales deben estar centrados a la “0”tolerancia al tema de Corrupción.
- ✓Ayuda a las empresas a crear una imagen profesional y a establecer una cultura ética sólida.



CTPAT Boletín

Julio 2020

La Importancia de un Código de Conducta

(Criterio 11.5)

Ultima actualización: Julio 1, 2020

El programa Alianza Aduana-Sector Privado Contra el Terrorismo (CTPAT) es parte de la estrategia de seguridad que Aduanas y Protección Fronteriza de los Estados Unidos (CBP) implementó a raíz de los ataques terroristas del 11 de septiembre del 2001. A través de este programa, CBP trabaja con la comunidad comercial para fortalecer las cadenas de suministro internacionales y mejorar la seguridad fronteriza de los Estados Unidos.

Este Boletín del programa aborda la importancia de contar con un Código de Conducta y brinda orientación a los Miembros sobre cómo cumplir con este importante requisito de seguridad del personal. Comencemos con lo que el criterio mínimo de seguridad 11.5 establece:

Criterio: Los miembros de CTPAT deben tener un Código de Conducta del Empleado que incluya expectativas y defina comportamientos aceptables. Las sanciones y los procedimientos disciplinarios deben incluirse en el Código de Conducta. Los empleados / contratistas deben reconocer que han leído y entendido el Código de Conducta al firmarlo, y este reconocimiento debe mantenerse en el archivo del empleado para la documentación.

Guía de implementación: Un Código de Conducta ayuda a proteger su negocio e informa a los empleados de las expectativas. Su propósito es desarrollar y mantener un estándar de conducta aceptable para la empresa. Ayuda a las empresas a desarrollar una imagen profesional y a establecer una cultura ética fuerte. Incluso hasta una pequeña empresa necesita tener un Código de Conducta; sin embargo, no necesita ser elaborado en diseño o contener información compleja.

¿Qué es un Código de Conducta? Un Código de Conducta es un documento importante de la compañía que describe cómo se espera que se comporten sus empleados. Un Código de Conducta rige las acciones: es un conjunto de reglas documentadas a las que los empleados y otras partes interesadas pueden hacer referencia para garantizar que se desempeñen en sus puestos según lo previsto por la empresa. El personal temporal y de medio tiempo, no solo los empleados, debe cumplir con el Código de Conducta.

El Código de Conducta de una empresa debe describir claramente lo que cree como organización, cómo cada empleado debe tratarse entre sí y las personas con las que interactúan como representantes de su negocio. Los códigos deben proporcionar un conjunto muy claro de expectativas sobre qué acciones son necesarias, aceptables o prohibidas.

Si bien la ley exige que las compañías públicas tengan un Código de Conducta, CTPAT exige que todas sus compañías Miembros lo hagan.

Finalmente, la aplicación del código es de importancia crítica. Todos en una organización, de arriba hacia abajo, deben rendir cuentas y aquellos que violen el Código de Conducta de la empresa deben enfrentar medidas disciplinarias. El código, por lo tanto, debe estar respaldado por sanciones y procedimientos disciplinarios.

U.S. Customs and Border Protection

Page 1

CTPAT

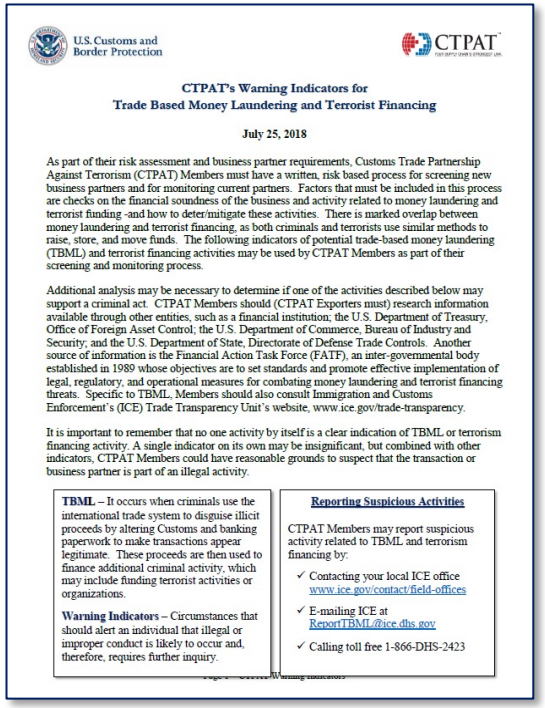
Beneficios – Ayuda a Crear y Mantener Una Cultura de Seguridad

- Fomenta el comportamiento ético.
- Hace de su empresa un mejor lugar para trabajar. Los empleados pueden usar el código como referencia y como guía, educándolos y capacitándolos para tomar las decisiones correctas a medida que enfrentan desafíos éticos.
- Desde una perspectiva de marketing, un código sirve como una declaración pública de los valores y principios de una empresa y de su compromiso con altos estándares y conducta.
- Ayuda a respaldar el compromiso de una empresa con la integridad y la seguridad de la cadena de suministro internacional.
- Promueve confianza entre los socios comerciales y otros stakeholders (partes interesadas). Una empresa que comunica su compromiso a la conducta ética y vela por su cumplimiento, crea un circulo virtuoso de empresas leales y con iguale principios.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Recursos

- Donde? Portal de CTPAT – Public Library Public Documents
- Que Clase de Recursos? PowerPoints / Boletínes / White Papers
- En Español? Sí - Algunos Están Disponibles en Español
- Usar Recursos en sus Propias Capacitaciones



U.S. Customs and Border Protection — CTPAT

CTPAT's Warning Indicators for Trade Based Money Laundering and Terrorist Financing

July 25, 2018

As part of their risk assessment and business partner requirements, Customs Trade Partnership Against Terrorism (CTPAT) Members must have a written, risk based process for screening new business partners and for monitoring current partners. Factors that must be included in this process are checks on the financial soundness of the business and activity related to money laundering and terrorist funding -and how to deter/mitigate these activities. There is marked overlap between money laundering and terrorist financing, as both criminals and terrorists use similar methods to raise, store, and move funds. The following indicators of potential trade-based money laundering (TBML) and terrorist financing activities may be used by CTPAT Members as part of their screening and monitoring process.

Additional analysis may be necessary to determine if one of the activities described below may support a criminal act. CTPAT Members should (CTPAT Exporters must) research information available through other entities, such as a financial institution; the U.S. Department of Treasury, Office of Foreign Asset Control; the U.S. Department of Commerce, Bureau of Industry and Security; and the U.S. Department of State, Directorate of Defense Trade Controls. Another source of information is the Financial Action Task Force (FATF), an inter-governmental body established in 1989 whose objectives are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering and terrorist financing threats. Specific to TBML, Members should also consult Immigration and Customs Enforcement's (ICE) Trade Transparency Unit's website, www.ice.gov/trade-transparency.

It is important to remember that no one activity by itself is a clear indication of TBML or terrorism financing activity. A single indicator on its own may be insignificant, but combined with other indicators, CTPAT Members could have reasonable grounds to suspect that the transaction or business partner is part of an illegal activity.

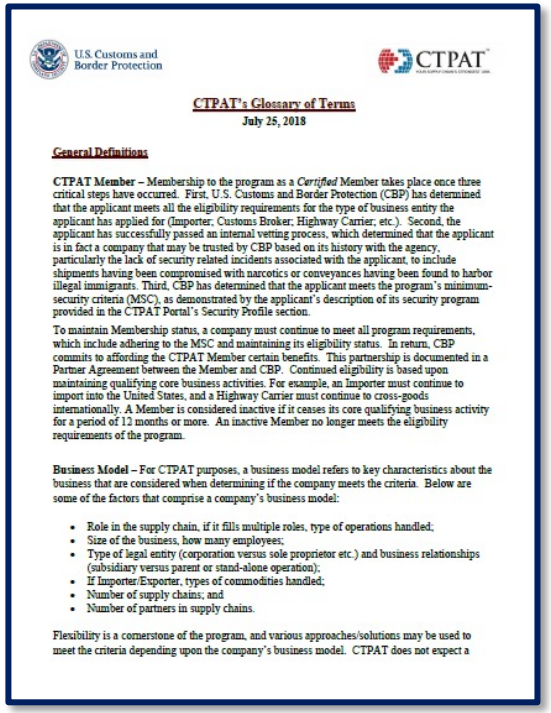
TBML – It occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

Warning Indicators – Circumstances that should alert an individual that illegal or improper conduct is likely to occur and, therefore, requires further inquiry.

Reporting Suspicious Activities

CTPAT Members may report suspicious activity related to TBML and terrorism financing by:

- ✓ Contacting your local ICE office www.ice.gov/contact/field-offices
- ✓ E-mailing ICE at ReportTBML@ice.dhs.gov
- ✓ Calling toll free 1-866-DHS-2423



U.S. Customs and Border Protection — CTPAT

CTPAT's Glossary of Terms

July 25, 2018

General Definitions

CTPAT Member – Membership to the program as a *Certified* Member takes place once three critical steps have occurred. First, U.S. Customs and Border Protection (CBP) has determined that the applicant meets all the eligibility requirements for the type of business entity the applicant has applied for (Importer; Customs Broker; Highway Carrier; etc.). Second, the applicant has successfully passed an internal vetting process, which determined that the applicant is in fact a company that may be trusted by CBP based on its history with the agency, particularly the lack of security related incidents associated with the applicant, to include shipments having been compromised with narcotics or conveyances having been found to harbor illegal immigrants. Third, CBP has determined that the applicant meets the program's minimum-security criteria (MSC), as demonstrated by the applicant's description of its security program provided in the CTPAT Portal's Security Profile section.

To maintain Membership status, a company must continue to meet all program requirements, which include adhering to the MSC and maintaining its eligibility status. In return, CBP commits to affording the CTPAT Member certain benefits. This partnership is documented in a Partner Agreement between the Member and CBP. Continued eligibility is based upon maintaining qualifying core business activities. For example, an Importer must continue to import into the United States, and a Highway Carrier must continue to cross-goods internationally. A Member is considered inactive if it ceases its core qualifying business activity for a period of 12 months or more. An inactive Member no longer meets the eligibility requirements of the program.

Business Model – For CTPAT purposes, a business model refers to key characteristics about the business that are considered when determining if the company meets the criteria. Below are some of the factors that comprise a company's business model:

- Role in the supply chain, if it fills multiple roles, type of operations handled;
- Size of the business, how many employees;
- Type of legal entity (corporation versus sole proprietor etc.) and business relationships (subsidiary versus parent or stand-alone operation);
- If Importer/Exporter, types of commodities handled;
- Number of supply chains; and
- Number of partners in supply chains.

Flexibility is a cornerstone of the program, and various approaches/solutions may be used to meet the criteria depending upon the company's business model. CTPAT does not expect a

U.S. Customs and Border Protection

Southern Border Truck Pest Contamination

Trade Outreach

U.S. Customs and Border Protection — May 2018 — USDA

Plan de Acción – 9 Objetivos

- Impulsado por el Comisionado Adjunto de CBP
- Iniciativa a nivel de agencia liderada por el programa de CTPAT

1. Comité de Seguridad Marítima y Portuaria
2. Reconocimiento de CTPAT a Compañía Certificada BASC
3. Acceso de CBP las Bases de Dato del WBO
4. Intercambio de Inteligencia e Información
5. Capacitación y Alcances
6. Licencia al WBO Para el Uso del Logotipo de CTPAT
7. Comité de Seguridad de la Cadena Logística
8. Presencia de CBP en Reuniones Claves del WBO
9. Comunicaciones Coordinadas

Trabajando Hacia Objetivos Comunes

- Internacionalizar criterios de seguridad importantes para las Aduanas y otras entidades de control fronterizo.
- Trabajar juntos, alineados bajos conceptos comunes y así darle facilitación a nuestro comercio.
- Firmando Acuerdos de Reconocimiento Mutuo basados en criterios que para la región son cruciales: protegen nuestros recursos naturales y nos dan competitividad a nivel global
- Exigiendo y demostrándole al resto del mundo que si se pueden implementar estos tipos de criterios de seguridad., que los programas OEA deben y pueden evolucionar.
- Liderando como región a nivel mundial y ante la Organización Mundial de Aduanas.
- Tener un campo de juego nivelado económicamente y que los consumidores de la región realmente sepan de dónde provienen sus productos y quien los hace.