DIPLOMADO EN

CERTIFICACIONES DE SEGURIDAD DE LA CADENA DE SUMINISTROS

A 10 años de la implementación de OEA en México.

CUEJ CENTRO UNIVERSITARIO DE ESTUDIOS JURÍDICOS PLANTEL BAJA CALIFORNIA

TLC ASOCIADOS

TRADE LAW & CUSTOMS

T&L Trade & Law College

Módulo VI

Seguridad física, controles de acceso y ciberseguridad

- Características de infraestructura de seguridad: CCTV, barda perimetral, alarmas, controles de acceso.
- Procesos de control de acceso
- Mantenimientos preventivos y correctivos

Ciberseguridad

- Asignación y retiro de equipos y cuentas de usuario
- Contraseñas y firewalls
- Análisis de vulnerabilidades de la red
- Concientización de riesgos para los usuarios
- Estándar NIST de CTPAT

Lic. Esmeralda Camacho

Especialista de Certificaciones y Seguridad en la Cadena de Suministro- OEA

2 –Seguridad Física

oea Operador Económico Autorizado MÉXICO

La empresa debe contar con **mecanismos** establecidos y **procesos** documentados para *impedir, detectar o disuadir* la entrada de personal no autorizado a las instalaciones.

Todas las áreas sensibles de la empresa deberán tener:

- barreras físicas
- elementos de control
- disuasión contra el acceso no autorizado

2.1 Instalaciones

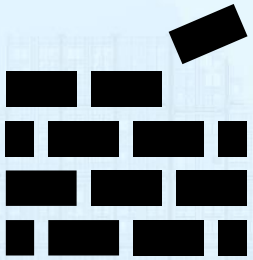
oea Operador Económico Autorizado MÉXICO

Las instalaciones deben estar construidas con materiales que puedan resistir accesos no autorizados.

Se deben realizar **inspecciones periódicas documentadas** para mantener la integridad de las estructuras y en el caso de haberse detectado una irregularidad, efectuar la *reparación correspondiente*.



2.1 Instalaciones



Materiales

Indicar los materiales predominantes con los que se encuentra construida la instalación

Señalar de que forma se lleva a cabo la revision y mantnimiento de la integridad de la estructura

Plano Arquitectónico

Plano donde se pueda identificar:

-Límites de las instalaciones

-Rutas de acceso

-Salidas de emergencia

-Ubicación de los edificios

2.2 Accesos en puertas y casetas

oea Operador Económico Autorizado ●● MÉXICO ●●

- Las puertas de entrada o salida de vehículos y/o personal deben ser **atendidas, controladas, vigiladas y/o supervisadas**. La cantidad de puertas de acceso debe mantenerse al mínimo necesario.

Indique cuantas puertas y/o accesos existen en las instalaciones, así como el horario de operación de cada una, e indique de qué forma son monitoreadas (en caso de tener personal asignado, indicar la cantidad).

Detalle si existen puertas y/o accesos bloqueados o permanentemente cerrados.

2.3 Bardas Perimetrales

oea Operador Económico Autorizado MÉXICO

Las bardas perimetrales y/o barreras periféricas deben instalarse para asegurar las instalaciones de la empresa, con *base en un análisis de riesgo*.
Se deben utilizar cercas, barreras interiores o un mecanismo para identificar y segregar:

- la carga internacional
- alto valor
- peligrosa

Las áreas de almacenaje, alto valor, peligrosas, y/o de acceso restringido, deben estar claramente identificadas y monitoreadas para prevenir ingresos no autorizados.

Estas deben ser inspeccionadas regularmente y llevar un registro de la revisión con la finalidad de asegurar su integridad e identificar daños.

2.3 Bardas Perimetrales

oea Operador Económico Autorizado ●●MÉXICO●●

Describa de qué manera se encuentra segregada la carga **destinada al extranjero, el material peligroso y la de alto valor**; asegúrese de incluir los siguientes puntos:

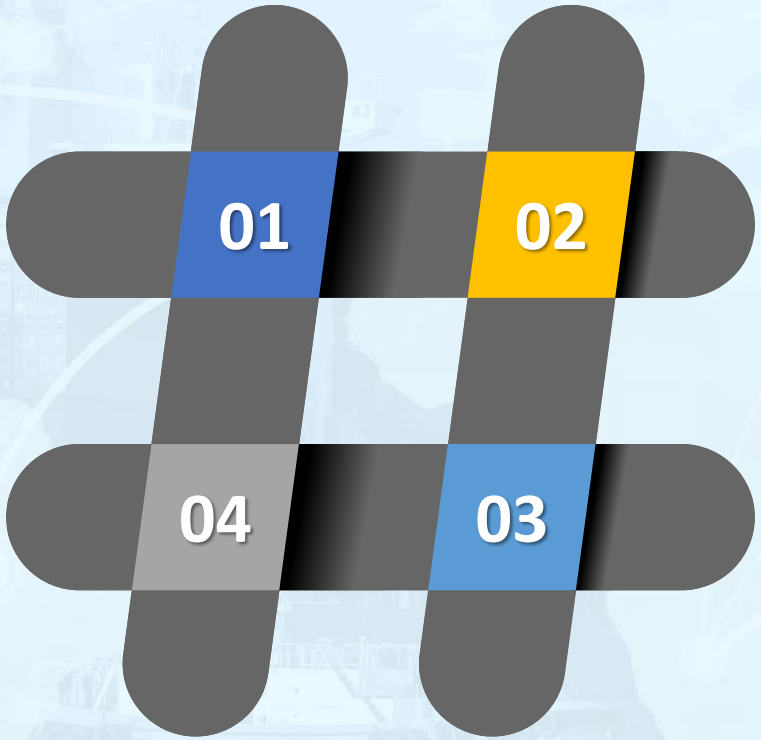
- Indique cómo separa la mercancía nacional y la de comercio exterior, y si está identificada de manera adicional (por ejemplo: empaque distinto, etiquetas, embalaje, entre otros).
- Identifique y señale las áreas de acceso restringido. (mercancías peligrosas, alto valor, confidenciales, etc.).

2.3 Bardas Perimetrales

oea Operador Económico Autorizado MÉXICO

El procedimiento para la inspección de las bardas perimétricas podría incluir:

Personal responsable para llevar a cabo el proceso



Cómo y con qué frecuencia se llevan a cabo las inspecciones de las cercas, bardas perimétricas y/o periféricas y los edificios.

Cómo se lleva el registro de la inspección.

Quién es el responsable de verificar que las reparaciones y/o modificaciones cumplan con las especificaciones técnicas y requisitos de seguridad necesarias


PRECAUCION

2.4 Estacionamientos

El acceso a los estacionamientos de las instalaciones debe ser **controlado y monitoreado**. Se debe prohibir que los *vehículos privados* (de empleados, visitantes, proveedores, contratistas, entre otros), se *estacionen dentro de las áreas de manejo y almacenaje de la mercancía*, así como en áreas adyacentes.

2.4 Estacionamientos

oea Operador Económico Autorizado MÉXICO

El procedimiento para el control y monitoreo de los estacionamientos debe incluir:

- Responsables de controlar y monitorear el acceso a los estacionamientos
- Políticas o mecanismos para no permitir el ingreso de vehículos privados a las áreas de almacenaje y manejo de mercancía.

- Identificación de los estacionamientos
- Cómo se lleva el control de entrada y salida de vehículos a las instalaciones. (Registros y mecanismos de control)

2.5 Control de Llaves y Dispositivos de Cerraduras

Las ventanas, puertas, así como las cercas interiores y exteriores, de acuerdo a su análisis de riesgo, deben asegurarse con dispositivos de cierre. La empresa debe contar con un procedimiento documentado para el manejo y control de llaves y/o dispositivos de cierre de las áreas interiores que se hayan considerado como críticas.

Asimismo, deben llevar un *registro* y establecer *cartas responsivas firmadas* de las personas que cuentan con llaves o accesos autorizados conforme a su nivel de responsabilidad y labores dentro de su área

oea Operador Económico Autorizado MÉXICO

2.5 Control de Llaves y Dispositivos de Cerraduras

Indique si todas las puertas, ventanas, entradas interiores y exteriores disponen de mecanismos de cierre o seguridad.

Señalar si existen áreas en las que se acceda con dispositivos electrónicos y/o algún otro mecanismo de acceso.

Procedimiento documentado para el manejo y control de llaves y/o dispositivos de cierre debe incluir:

- Tratamiento de pérdida o no devolución de llaves.
- Formato y/o registro de control para el préstamo de llaves
- Responsables de administrar y controlar la seguridad de las llaves

oea Operador Económico Autorizado MÉXICO

2.6 Alumbrado

oea Operador Económico Autorizado MÉXICO

El alumbrado dentro y fuera de las instalaciones debe permitir una clara identificación de personas, material y/o equipo que ahí se encuentre, incluyendo las siguientes áreas: entradas y salidas, áreas de manejo y almacenaje de la mercancía, bardas perimetrales y/o periféricas, cercas interiores y áreas de estacionamiento, debiendo contar con un sistema de emergencia y/o respaldo en las áreas sensibles.

Señale qué áreas se encuentran iluminadas y cuáles cuentan con un sistema de respaldo (indique si cuenta con una planta de poder auxiliar o algún otro mecanismo para suministrar energía eléctrica en caso de alguna contingencia)

De qué manera se cerciora que el sistema de iluminación sea el apropiado en cada una de las áreas de la empresa, de manera que permita una clara identificación del personal, material y/o equipo que ahí se encuentra

1. Responsable del control de los sistemas de iluminación.
2. Cómo se controla el sistema de iluminación.
3. Horarios de funcionamiento.
4. Identificación de áreas con iluminación permanente.
5. Programa de mantenimiento y revisión.

2.7 Aparatos de Comunicación

oea Operador Económico Autorizado MÉXICO

La empresa debe contar con aparatos y/o sistemas de comunicación con la finalidad de contactar de forma inmediata al personal de seguridad y/o con las autoridades, en caso de ocurrir una situación de emergencia y seguridad. Adicionalmente, se debe contar con un sistema de respaldo y verificar su buen funcionamiento de manera periódica.

Procedimiento que el personal debe realizar para contactar al personal de seguridad de la empresa o, en su caso, de la autoridad correspondiente.

Indicar si el personal operativo y administrativo cuenta o dispone de aparatos (teléfonos fijos, móviles, botones de alerta y/o emergencia, etc.), para comunicarse con el personal de seguridad y/o con quien corresponda

Indique qué tipo de aparatos de comunicación utiliza el personal de seguridad en la empresa (teléfonos fijos, celulares, radios, sistema de alarma, etc.).

2.7 Aparatos de Comunicación

oea Operador Económico Autorizado ●● MÉXICO ●●

Responsable del buen funcionamiento y mantenimiento de los aparatos de comunicación.

Registro de verificación y mantenimiento de los aparatos

Forma de asignación de los aparatos de comunicación

Políticas de asignación de aparatos de comunicación móvil.

Programa de mantenimiento de aparatos de comunicación fija y móvil.

Aparatos de comunicación de respaldo, en caso de que el sistema permanente fallara

Contáctanos: desarrollo.academico@tradelawcollege.edu.mx Tel. (664) 200 2770 Cel. (663) 167 2862 www.tradelawcollege.edu.mx

2.8 Sistema de Alarma y CCTV

Los sistemas de alarmas y de circuito cerrado de televisión (CCTV), se deben **utilizar para vigilar, notificar o disuadir accesos no autorizados y actividades prohibidas** en las instalaciones y notificar al área correspondiente, además de utilizarse como herramienta de prueba en investigaciones derivadas de algún incidente de seguridad.

Estos sistemas deberán colocarse de acuerdo a un análisis de riesgo previo, de tal forma que se mantengan vigiladas y monitoreadas las *áreas que impliquen el manejo y almacenaje de las mercancías, materias primas y materiales de empaque, inspecciones de seguridad a los vehículos de carga, así como del acceso de personal, visitantes, proveedores, vehículos de pasajeros y de carga.*

oea Operador Económico Autorizado MÉXICO

2.8 Sistema de Alarma y CCTV

Dichos sistemas deben permitir una clara identificación del área o ambiente que vigila

oea Operador Económico Autorizado MÉXICO


2018-10-2


2018-12-10 13:41:07
0285

Errores en el CCTV

CORRECTA COLOCACIÓN DEL SISTEMA CCTV

2.8 Sistema de Alarma y CCTV

Estar permanentemente grabando y mantener un respaldo de las grabaciones por lo menos de un mes, considerando que, en el caso de que sus procesos logísticos excedan este periodo, deberá aumentar el periodo del mantenimiento de estos respaldos, con la finalidad de tener los elementos necesarios para destinar responsabilidades en caso de un incidente de seguridad.

De manera de lo posible, contar con una fuente de energía alterna para el correcto funcionamiento en caso de algún problema con el suministro principal

OEA-30 días

CTPAT-14 días después de llegar a destino

oea Operador Económico Autorizado MÉXICO

2.8 Sistema de Alarma y CCTV

El sistema de CCTV, debe contar con un procedimiento documentado de operación que incluya:

- La supervisión del buen estado del equipo
- Frecuencia con la que debe realizar el respaldo de las grabaciones
- La verificación de la correcta posición de las cámaras
- Responsables de su operación

Dicho sistema deberá tener un acceso restringido.

2.8 Sistema de Alarma y CCTV

Información a indicar en el perfil:

- Indique el número de cámaras de CCTV instaladas, y su ubicación por áreas. (Detallar si cubre áreas críticas)
- Señale la ubicación del sistema de CCTV, dónde se localizan los monitores, quién los revisa, así como los horarios de operación, y en su caso, si existen estaciones de monitoreo remoto.
- Indique de qué forma revisan las grabaciones. (Aleatoria, cada semana, eventos especiales, áreas restringidas, etc.).
- Indique por cuánto tiempo se mantienen estas grabaciones.
- Indique si el sistema de CCTV se encuentra respaldado por una planta de poder eléctrica o algún otro mecanismo para suministrar energía eléctrica.

- Servicio central de alarmas externas
-Si las puertas y ventanas tienen sensores de alarma, así como las áreas donde se cuenta con sensores de movimiento.
-Procedimiento a seguir en caso de activarse una alarma.

oea Operador Económico Autorizado MÉXICO

9. Seguridad Física

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

ID	Criterios	Guía de la implementación
9.1	Todas las instalaciones para el almacenamiento y la manipulación de la carga, incluidos los patios de remolques y las oficinas, deben tener barreras físicas o elementos de disuasión que impidan el acceso no autorizado.	
9.2	Las cercas perimetrales deberían encerrar las áreas alrededor de las instalaciones para el almacenamiento y la manipulación de la carga. Si una instalación manipula carga, se deberían usar cercas interiores para proteger la carga y las áreas de manipulación de la carga. Según el riesgo, un cercado interior adicional debería separar los varios tipos de carga, como los materiales locales, internacionales, de alto valor o peligrosos. Las cercas deberían ser inspeccionadas periódicamente por personal designado para comprobar la integridad de las mismas y que no tengan daños. Si se encuentran daños en la cerca, las reparaciones deberían hacerse lo antes posible.	Se pueden utilizar otras barreras aceptables en lugar de cercas, como un muro divisorio o elementos naturales que sean impenetrables o que, de otra forma, impidan el acceso, como un acantilado empinado o matorrales densos.
9.4	Las puertas por donde los vehículos o el personal entran o salen (así como otros puntos de salida) deben ser reforzadas o vigiladas. Las personas y los vehículos pueden estar sujetos a inspecciones de acuerdo con las leyes locales y laborales.	Se recomienda que el número de puertas se mantenga al mínimo necesario para el acceso y la seguridad adecuados. Otros puntos de salida serían las entradas a las instalaciones que no están cercadas.

9.5	Se debería prohibir que los vehículos de pasajeros privados se estacionen en las áreas de almacenamiento y manipulación de la carga, y de los medios de transporte, o en zonas adyacentes.	Ubique las áreas de estacionamiento fuera de las áreas cercadas u operativas, o al menos a distancias significativas de las áreas de almacenamiento y manipulación de la carga.
9.6	Se debe proporcionar una iluminación adecuada dentro y fuera de las instalaciones, incluidas, según corresponda, las siguientes áreas: las entradas y las salidas, las áreas de almacenamiento y manipulación de carga, las líneas de las cercas y las áreas de estacionamiento.	Los temporizadores automáticos o los sensores de luz que encienden automáticamente las luces de seguridad apropiadas son complementos útiles a los aparatos de iluminación.
9.7	La tecnología de seguridad debería utilizarse para vigilar las instalaciones y evitar el acceso no autorizado a las áreas sensibles.	La tecnología de seguridad electrónica utilizada para proteger o vigilar áreas sensibles y puntos de acceso incluye: sistemas de alarma contra robo (perímetro e interior), también conocidos como sistemas de detección de intrusos (IDS); dispositivos de control de acceso y sistemas de videovigilancia (VSS), incluidas las cámaras de circuito cerrado de televisión (CCTV). Un sistema CCTV / VSS podría incluir componentes como cámaras analógicas (de cable coaxial), cámaras basadas en el protocolo de Internet (IP) (de red), dispositivos de grabación y software de gestión de video. Las áreas protegidas o sensibles que se beneficiarían de la videovigilancia pueden incluir: las áreas de almacenamiento y manipulación de la carga, las áreas de envío y recepción donde se conservan los documentos de importación, los servidores de TI, los patios y áreas de almacenamiento para los Instrumentos de Tráfico Internacional (IIT), las áreas donde los IIT se inspeccionan y las áreas de almacenamiento de sellos.

9.8	Los miembros que dependen de la tecnología de seguridad para la seguridad física deben tener políticas y procedimientos escritos que rijan el uso, el mantenimiento y la protección de esta tecnología.	La tecnología de seguridad necesita probarse periódicamente para garantizar su funcionamiento correcto. Existen directrices generales a seguir:
	Como mínimo, estas políticas y procedimientos deben estipular: • Que el acceso a los lugares donde se controla o administra la tecnología se restringe al personal autorizado; • Los procedimientos que se han implementado para probar o inspeccionar la tecnología de manera periódica; • Que las inspecciones incluyen verificaciones de que todo el equipo funciona correctamente y, si corresponde, que el equipo está colocado correctamente; • Que los resultados de las inspecciones y pruebas de desempeño estén documentados; • Que, si las acciones correctivas son necesarias, estas se implementen lo antes posible y que las acciones correctivas tomadas estén documentadas; • Que los resultados documentados de estas inspecciones se conserven durante un tiempo prudencial para fines de auditoría. Si se utiliza una estación de vigilancia central subcontratada (fuera del sitio), el miembro de CTPAT debe contar con procedimientos escritos que estipulen la funcionalidad de los sistemas críticos y los protocolos de autenticación, entre ellos los cambios en el código de seguridad, sumando o restando personal autorizado, las revisiones de contraseña y el acceso o el rechazo a los sistemas. Las políticas y procedimientos de tecnología de seguridad se deben revisar y actualizar anualmente, o con mayor frecuencia, según lo dicte el riesgo o las circunstancias.	• Probar los sistemas de seguridad después de cualquier trabajo de servicio y durante y después de reparaciones, modificaciones o adiciones importantes a un edificio o instalación. El componente de un sistema puede haber sido comprometido, ya sea intencionalmente o no. • Probar los sistemas de seguridad después de cualquier cambio importante en los servicios telefónicos o de internet. Cualquier aspecto que pueda afectar la capacidad del sistema para comunicarse con el centro de vigilancia merece ser revisado con atención. • Asegurarse de que la configuración de video se haya hecho correctamente: grabación activada por movimiento; alertas por detección de movimiento; imágenes por segundo (IPS) y nivel de calidad. • Asegurarse de que los lentes de la cámara (o los domos que protegen las cámaras) estén limpios y que los lentes estén enfocados. La visibilidad no debería estar limitada por obstáculos o luces brillantes. • Hacer pruebas para asegurarse de que las cámaras de seguridad estén colocadas correctamente y permanezcan en la posición correcta (las cámaras pudieron haber sido movidas deliberada o accidentalmente).

9.9	Los miembros de CTPAT deberían utilizar recursos con licencia o certificados al considerar el diseño y la instalación de la tecnología de seguridad.	La tecnología de seguridad de hoy día es compleja y evoluciona rápidamente. Muchas veces las empresas compran tecnología de seguridad inadecuada que demuestra ser ineficaz cuando se requiere o pagan más de lo necesario. Buscar la orientación calificada ayudará al comprador a seleccionar las opciones tecnológicas adecuadas para sus necesidades y presupuesto. Según la Asociación Nacional de Contratistas Eléctricos (NECA), en los EE. UU., 33 estados actualmente tienen requisitos de licencia para profesionales dedicados a la instalación de sistemas de seguridad y alarmas.
9.10	Toda la infraestructura de la tecnología de seguridad debe asegurarse físicamente para evitar el acceso no autorizado.	La infraestructura de la tecnología de seguridad incluye las computadoras, el software de seguridad, los paneles de control electrónico, las cámaras de circuito cerrado de televisión o videovigilancia, los componentes de energía eléctrica y disco duro para cámaras, así como las grabaciones.
9.11	Los sistemas de la tecnología de seguridad deberían configurarse con una fuente de energía alternativa que permita que los sistemas continúen funcionando en caso de una pérdida inesperada de energía directa.	Un delincuente que trata de violar su seguridad puede intentar desactivar la electricidad de su tecnología de seguridad para circunnavegarla. Por lo tanto, es importante tener una fuente de energía alternativa para su tecnología de seguridad. Una fuente de energía alternativa puede ser una fuente de generación de energía auxiliar o baterías de respaldo. Los generadores de energía de respaldo también se pueden usar para otros sistemas importantes como la iluminación.

9.12	Si se hace uso de sistemas de cámaras, las cámaras deberían vigilar las instalaciones y las áreas sensibles para evitar el acceso no autorizado. Las alarmas deberían usarse para alertar a una empresa sobre el acceso no autorizado a áreas sensibles.	Las áreas sensibles, según corresponda, pueden incluir las áreas de almacenamiento y manipulación de la carga, las áreas de envío y recepción donde se conservan los documentos de importación, los servidores de TI, los depósitos de contenedores y las áreas de almacenamiento para los Instrumentos de Tráfico Internacional (IIT), las áreas donde se inspeccionan los IIT y las áreas de almacenamiento de los sellos.
9.13	Si se hace uso de sistemas de cámaras, las cámaras deben colocarse de forma que cubran áreas clave de las instalaciones que conciernen al proceso de importación o exportación. Las cámaras deberían programarse para grabar a la más alta calidad de imagen razonablemente disponible, y configurarse para grabar las 24 horas del día, los siete días de la semana.	Posicionar las cámaras correctamente es importante para permitir que las cámaras graben tanto como sea posible de la "cadena de custodia" física dentro del control de la instalación. Según el riesgo, las áreas clave pueden incluir el almacenamiento y manipulación de la carga; el envío y la recepción; el proceso de carga, el proceso de sellado; la llegada y salida de los medios de transporte; los servidores de TI; las inspecciones (de seguridad y agrícolas) de los contenedores; el almacenamiento de los sellos y cualquier otra área relacionada con la seguridad de los cargamentos internacionales.
9.14	Si se hace uso de los sistemas de cámaras, las cámaras deberían tener una función de alarma o notificación, lo que señalaría que hay una "falla de operación o grabación".	Una falla en los sistemas de videovigilancia podría ser el resultado de que alguien desactive el sistema para violar una cadena de suministro sin dejar prueba en video de la infracción. La función de falla en la operación puede provocar que se envíe una notificación electrónica a las personas previamente designadas indicándoles que el dispositivo requiere atención inmediata.

9.15	Si se hace uso de sistemas de cámaras, se deben realizar revisiones aleatorias periódicas de las imágenes de las cámaras (por parte de la administración, la seguridad u otro personal designado) para verificar que los procedimientos de seguridad de la carga se están siguiendo adecuadamente de acuerdo con la ley. Los resultados de las revisiones deben resumirse por escrito para incluir cualquier acción correctiva tomada. Los resultados se deben conservar durante un tiempo prudencial para fines de auditoría.	Si las imágenes de la cámara solo se revisan con causa (como parte de una investigación luego de una violación de seguridad u otros), no se está haciendo uso del beneficio completo que genera la posesión de cámaras. Las cámaras no son solamente herramientas de investigación; si se utilizan de una manera dinámica, pueden ayudar a evitar que ocurra una violación de la seguridad desde el comienzo mismo. El enfoque debe estar en la revisión aleatoria de las imágenes en la cadena de custodia física para garantizar que el cargamento permaneció seguro y que se siguieron todos los protocolos de seguridad. Algunos ejemplos de los procesos que pueden revisarse son los siguientes: • Las actividades de manipulación de la carga; • Las inspecciones de los contenedores; • El proceso de carga; • El proceso de sellado; • La llegada y salida de los medios de transporte; y • La salida de la carga y otros. **Propósito de la revisión:** La revisión es para evaluar el cumplimiento y la eficacia en general de los procesos de seguridad establecidos, para identificar brechas o debilidades percibidas, y para establecer acciones correctivas para respaldar la mejoría de los procesos de seguridad. Según el riesgo (incidentes anteriores o un informe anónimo sobre un empleado que no sigue los protocolos de seguridad en el muelle de carga u otros), el miembro puede fijar periódicamente una revisión.

Asuntos que deben incluirse en el resumen escrito:

- La fecha de la revisión;
- La fecha en que se revisaron las imágenes;
- La cámara o el área de donde procede la grabación
- Una breve descripción de cualquier hallazgo; y
- Las acciones correctivas, si se justifican.

9.16	Si se utilizan cámaras, se deberían conservar las grabaciones de imágenes que cubren procesos clave de importación o exportación de un cargamento vigilado durante suficiente tiempo para que se pueda completar una investigación.	Si se produjera una violación, sería necesario llevar a cabo una investigación, y conservar todas las imágenes de las cámaras que cubrían el embalado (para exportación) y los procesos de carga o sellado serían de suma importancia para descubrir dónde se pudo haber comprometido la cadena de suministro. El programa CTPAT recomienda asignar al menos 14 días después de que el cargamento vigilado haya llegado al primer punto de distribución, donde el contenedor se abre por primera vez después del despacho aduanero.

Actividad

Kahoot

DIPLOMADO EN

CERTIFICACIONES DE SEGURIDAD DE LA CADENA DE SUMINISTROS

A 10 años de la implementación de OEA en México.

CUEJ CENTRO UNIVERSITARIO DE ESTUDIOS JURÍDICOS PLANTEL BAJA CALIFORNIA

TLC ASOCIADOS

TRADE LAW & CUSTOMS

T&L Trade & Law College

Módulo VI

Seguridad física, controles de acceso y ciberseguridad

- Características de infraestructura de seguridad: CCTV, barda perimetral, alarmas, controles de acceso.
- Procesos de control de acceso
- Mantenimientos preventivos y correctivos

Ciberseguridad

- Asignación y retiro de equipos y cuentas de usuario
- Contraseñas y firewalls
- Análisis de vulnerabilidades de la red
- Concientización de riesgos para los usuarios
- Estándar NIST de CTPAT

Lic. Esmeralda Camacho

Especialista de Certificaciones y Seguridad en la Cadena de Suministro- OEA

Controles de Acceso Físico

Los controles de acceso físico, son **mecanismos o procedimientos que previenen e impiden la entrada no autorizada a las instalaciones**, mantienen control del ingreso de los empleados, visitantes y proveedores, además de proteger los bienes de la empresa.

Los controles de acceso deben incluir la identificación de todos los empleados, visitantes y proveedores en todos los puntos de entrada. Así mismo, se deben mantener *registros* y evaluar permanentemente los mecanismos o procedimientos documentados de ingreso a las instalaciones, siendo la base para comenzar a integrar la seguridad como una de las funciones primordiales dentro de cualquier empresa.

3.1 Personal de Seguridad

La empresa debe contar con personal de seguridad y vigilancia. Este personal desempeña *un rol importante en la protección física de las instalaciones y de la mercancía durante su traslado, manejo y resguardo dentro de la empresa, así como para controlar el acceso y salida de todas las personas al inmueble.*

El personal de seguridad, deberá contar con un procedimiento documentado para llevar a cabo sus funciones y tener pleno conocimiento de los mecanismos y procedimientos en situaciones de emergencia, detección de personas no autorizadas o cualquier incidente de seguridad en la instalación.

3.1 Personal de Seguridad

Describa el procedimiento documentado para la operación del personal de seguridad debe incluir:

Indique el número del personal de seguridad que labora en la empresa.

Señale los cargos y/o funciones del personal y horarios de operación.

Servicio externo, proporcionar los datos generales de la empresa, y especificar número del personal empleado, detalles de operación, registros y reportes que utilizan para desempeñar sus funciones.

En caso de contar con personal armado, describa el procedimiento para el control y resguardo de las armas.

3.2 Identificación de los Empleados

oea Operador Económico Autorizado MÉXICO

Debe existir un sistema de *identificación de empleados* con fines de acceso a las instalaciones. Los empleados sólo deben tener acceso a aquellas áreas que necesiten para desempeñar sus funciones. La gerencia o el personal de seguridad de la compañía deben controlar adecuadamente la entrega y devolución de insignias, gafetes y/o credenciales de identificación de empleados, visitantes y proveedores. Se deben documentar los procedimientos para la entrega, devolución y cambio de dispositivos de acceso (por ejemplo, llaves, gafetes y/o credenciales, tarjetas de proximidad, etc.).

- Procedimiento para la identificación de los empleados y asegúrese de incluir los siguientes puntos:

-Mecanismos de identificación (gafete y/o credencial con foto, control de acceso, biométricos, tarjetas de proximidad, etc.).

-Indique cómo se identifica al personal contratado por un socio comercial, que labore dentro de las instalaciones (contratistas, sub-contratados, servicios in house sub-maquila, etc.).

- Proceso de entrega, cambia y retira las identificaciones y controles de acceso del empleado y asegúrese de incluir las áreas responsables de autorizarlas y administrarlas.
- Procedimiento documentado para el control de las identificaciones.

3.3 Identificación de Visitantes y Proveedores

oea Operador Económico Autorizado MÉXICO

Para tener acceso a las instalaciones, los visitantes y proveedores deberán presentar identificación oficial con fotografía con fines de documentación a su llegada y se deberá llevar un registro. Todos los visitantes deberán estar acompañados por personal de la empresa durante su permanencia en las instalaciones y asegurarse que el visitante porte siempre en un lugar visible la identificación provisional proporcionada. Este procedimiento deberá estar documentado.

Describa el procedimiento para el control de acceso de los visitantes y proveedores, asegúrese de incluir los siguientes puntos:

- Señale qué registros se llevan a cabo (formatos personales por cada visita, bitácoras, entre otros).
- Señale quién es la persona responsable de acompañar al visitante y/o proveedor y si existen áreas restringidas para su ingreso.

oea Operador Económico Autorizado MÉXICO

3.3 Identificación de Visitantes y Proveedores

Para tener acceso a las instalaciones, los visitantes y proveedores deberán presentar identificación oficial con fotografía con fines de documentación a su llegada y se deberá llevar un registro. Todos los visitantes deberán estar acompañados por personal de la empresa durante su permanencia en las instalaciones y asegurarse que el visitante porte siempre en un lugar visible la identificación provisional proporcionada.

Este procedimiento deberá estar documentado.

Describa el procedimiento para el control de acceso de los visitantes y proveedores, asegúrese de incluir los siguientes puntos:

- Señale qué registros se llevan a cabo (formatos personales por cada visita, bitácoras, entre otros).
- Señale quién es la persona responsable de acompañar al visitante y/o proveedor y si existen áreas restringidas para su ingreso.

3.4 Procedimiento de Identificación y Retiro de Personas o Vehículos no Autorizados

La empresa debe contar con procedimientos documentados que especifiquen como identificar, enfrentar o reportar a personas y/o vehículos no autorizados o identificados, dicho procedimiento debe ser comunicado al personal responsable mediante capacitación. La capacitación debe estar documentada.

Anexe el procedimiento documentado para identificar, enfrentar o reportar personas y/o vehículos no autorizados o identificados.

El procedimiento deberá incluir:

a) Personal responsable.
b) Designar a una persona o área responsable para ser informado de los incidentes de seguridad.
c) Indicaciones para enfrentar y dirigirse al personal no identificado.
d) Señalar en qué casos deberá reportarse a las autoridades correspondientes.
e) Cómo se lleva a cabo el registro de los incidentes de seguridad y las medidas adoptadas en cada caso.

oea Operador Económico Autorizado ●●MÉXICO●●

10. Controles de Acceso

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

ID	Criterios	Guía de la implementación
10.1	Los miembros de CTPAT deben tener procedimientos por escrito que regulen cómo se otorgan, cambian y retiran las credenciales de identificación y los dispositivos de acceso. Cuando corresponda, debe existir un sistema de identificación de personal para fines de identificación positiva y control de acceso. El acceso a las áreas sensibles debe restringirse según la descripción del trabajo o las tareas asignadas. El retiro de los dispositivos de acceso debe llevarse a cabo tras la separación del empleado de la empresa.	Los dispositivos de acceso incluyen las credenciales de identificación para los empleados, las credenciales temporales para visitantes y proveedores, los sistemas de identificación biométrica, tarjetas de proximidad, los códigos y las claves. Cuando se separa a los empleados de una empresa, el uso de listas de control de salida ayuda a asegurar que todos los dispositivos de acceso hayan sido devueltos o desactivados. Para las empresas más pequeñas, donde el personal se conoce, no se requiere ningún sistema de identificación. En general, para una empresa con más de 50 empleados, se requiere un sistema de identificación.

ID	Criterios	Guía de la implementación
10.2	Los visitantes, vendedores y proveedores de servicios deben presentar una identificación con fotografía a su llegada, y se debe mantener una bitácora que registre los detalles de la visita. Todos los visitantes deberían ser escoltados. Además, todos los visitantes y proveedores de servicios deberían recibir una identificación temporal. Si se utiliza una identificación temporal, debe estar visible en todo momento durante la visita. La bitácora de registro debe incluir lo siguiente: • Fecha de la visita; • Nombre del visitante; • Verificación de una identificación con fotografía (del tipo verificado, como licencia de conducir o tarjeta nacional de identidad). Los visitantes frecuentes y conocidos, como los vendedores habituales, pueden pasar sin la identificación con fotografía, pero siempre se debe registrar su ingreso y salida de la instalación; • Hora de llegada; • Punto de contacto en la empresa; y • Hora de salida.	
10.3	Los conductores que entregan o reciben la carga deben identificarse positivamente antes de recibir o liberar la carga. Los conductores deben presentar una identificación con fotografía emitida por el gobierno al empleado de la instalación que otorgue acceso a fin de verificar su identidad. Si no es factible presentar una identificación con fotografía emitida por el gobierno, el empleado de la instalación puede aceptar una forma reconocible de identificación con fotografía emitida por la empresa transportista de carretera que emplea al conductor que recoge la carga.	

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

ID	Criterios	Guía de la implementación
10.4	Se debe mantener una bitácora de recolección de carga para registrar a los conductores y registrar los detalles de sus medios de transporte al recoger la carga. Cuando los conductores llegan para recoger la carga en una instalación, un empleado de la instalación debe registrarlos en la bitácora de recolección de carga. Cuando los conductores salen, se debe registrar su salida. La bitácora de carga debe mantenerse en un lugar seguro, y los conductores no deben tener acceso a la misma. La bitácora de recolección de carga debería incluir los siguientes puntos: • El nombre del conductor; • La fecha y la hora de llegada; • El patrono; • El número de camión; • El número de remolque; • La hora de salida; • El número del sello colocado al cargamento al momento de la salida.	Una bitácora de visitantes puede tener doble función como bitácora de carga, siempre que la información adicional esté registrada en la misma.

ID	Criterios	Guía de la implementación
10.7	Antes de la llegada, el transportista debería informar a la instalación la hora estimada de llegada para la recolección programada, el nombre del conductor y el número de camión. Cuando sea operacionalmente factible, los miembros de CTPAT deberían permitir entregas y recolecciones solamente con cita.	Este criterio ayudará a las expedidoras y a los transportistas a evitar las recolecciones ficticias. Las recolecciones ficticias son esquemas delictivos que dan lugar al robo de carga mediante el engaño, lo que incluye a choferes de camión que usan identificaciones falsas o comercios ficticios establecidos con el propósito de robar carga. Cuando un transportista cuenta con choferes fijos que recogen mercancías de una instalación determinada, una buena práctica es que esta mantenga una lista de los choferes con sus fotografías. Por lo tanto, si no es posible informar a la empresa qué chofer va a venir, la empresa aún podrá verificar que el conductor cuenta con la aprobación para recoger la carga de la instalación.
10.8	Antes de ser admitidos, los paquetes y el correo que lleguen deberían examinarse periódicamente en busca de tráfico ilegal.	Algunos ejemplos de este tráfico ilegal incluyen, entre otros, explosivos, drogas ilícitas y dinero.
10.10	Si se utilizan guardias de seguridad, las instrucciones de trabajo para los guardias de seguridad deben estar en las políticas y los procedimientos escritos. La administración debe verificar periódicamente el cumplimiento y la idoneidad de estos procedimientos mediante auditorías y revisiones de las políticas.	Si bien cualquier instalación puede emplear guardias, a menudo se emplean en las plantas de fabricación, los puertos marítimos, los centros de distribución, los patios de almacenamiento para los Instrumentos de Tráfico Internacionales, los centros consolidadores y expedidores.

DIPLOMADO EN
CERTIFICACIONES DE SEGURIDAD DE LA CADENA DE SUMINISTROS

A 10 años de la implementación de OEA en México.

CUEJ CENTRO UNIVERSITARIO DE ESTUDIOS JURÍDICOS PLANTEL BAJA CALIFORNIA

TLC ASOCIADOS

TRADE LAW & CUSTOMS

Trade & Law College

Ciberseguridad

- Asignación y retiro de equipos y cuentas de usuario
- Contraseñas y firewalls
- Análisis de vulnerabilidades de la red
- Concientización de Riesgos para Usuarios
- Esándar NIST

Jueves 27 Octubre 2022

Ciberseguridad

En el mundo digital de hoy, la ciberseguridad es la **clave** para **salvaguardar** los activos más preciados de la empresa: *la propiedad intelectual, la información de los clientes, los datos comerciales y financieros, y los registros de los empleados, entre otros*. Con una mayor conectividad a la internet existe el riesgo de una violación de los sistemas de información de la empresa. Esta amenaza atañe a empresas de todo tipo y tamaño. Las medidas para proteger la tecnología de la información (TI) y los datos de la empresa son de vital importancia, y los criterios indicados proporcionan una base para un programa general de ciberseguridad para los miembros.

Ciberseguridad

Se debe contar con **políticas o procedimientos** de ciberseguridad integrales y por escrito para proteger los sistemas de tecnología de la información (TI). La política escrita de TI debe cubrir, como mínimo, todos los criterios individuales de la ciberseguridad.

Para defender los sistemas de Tecnología de la Información de amenazas de ciberseguridad comunes, las empresas *deben instalar suficientes programas de software y equipos para protegerse de programas malignos* (virus, programas espías, gusanos y troyanos, etc.) y de intrusiones externas e internas (cortafuegos) en los sistemas de cómputo de los miembros.

Los miembros deben asegurarse de que su software de seguridad esté **actualizado y reciba actualizaciones de seguridad periódicas**. Los miembros deben contar con políticas y procedimientos para prevenir ataques a través de la ingeniería social. Si se da una filtración de datos u otro evento imprevisto provoca la pérdida de datos o equipo, los procedimientos deben incluir una recuperación (o reemplazo) de los sistemas o datos de TI

Ciberseguridad

Una red de cómputo segura es de suma importancia para una empresa y garantizar su protección requiere pruebas periódicas. Esto se puede hacer mediante la programación de **escaneos de vulnerabilidad**.

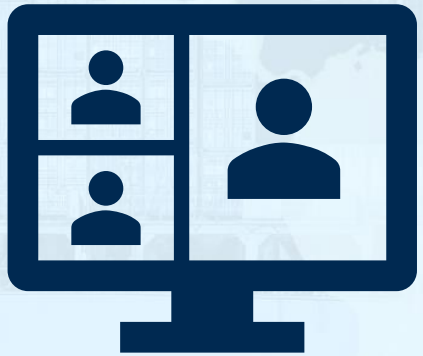
Un escaneo de la vulnerabilidad (VS) *identifica aberturas en sus computadoras* (puertos abiertos y direcciones IP), *sus sistemas operativos y el software a través del cual un pirata informático podría obtener acceso a los sistemas de TI de la empresa*.

El VS hace esto comparando los resultados de su análisis con los de una base de datos de vulnerabilidades conocidas y produce un informe de correcciones para que la empresa tome medidas.

La **frecuencia** de las pruebas dependerá de varios factores que incluyen el modelo de negocio y el nivel de riesgo de la empresa. Por ejemplo, se deben realizar pruebas cada vez que hay cambios en la infraestructura de la red de una empresa. No obstante, los ciberataques están aumentando entre empresas de todos los tamaños, y esto debe tomarse en consideración a la hora de diseñar un plan de pruebas.

Ciberseguridad

Las **políticas de ciberseguridad** deberían abordar cómo un miembro comparte información sobre amenazas de ciberseguridad con el gobierno y otros socios comerciales.



Se insta a los miembros a **compartir información** sobre amenazas de ciberseguridad con el gobierno y los socios comerciales dentro de la cadena de suministro.

El intercambio de información es una parte clave de la misión del Departamento de Seguridad Nacional para crear una conciencia situacional compartida de la actividad cibernética maliciosa.

El del Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC) comparte información entre socios del sector público y privado para crear conciencia sobre las vulnerabilidades, los incidentes y las mitigaciones. Los usuarios de sistemas de control cibernético e industrial pueden suscribirse a productos de información, fuentes (feeds) y servicios informáticos sin costo alguno.

Ciberseguridad

Debe existir un **sistema para identificar el acceso no autorizado** a los sistemas o datos de TI o el abuso de políticas y procedimientos, incluido el acceso inadecuado a los sistemas internos o sitios web externos y la manipulación o alteración de los datos comerciales por parte de los empleados o contratistas. Todos los infractores deben estar sujetos a las acciones disciplinarias correspondientes.

Phishing

Phishing es el delito de **engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito**. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. *Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo*. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.
Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

Phishing

Alerta C-TPAT por ciberamenazas en teletrabajo

TLC ASOCIADOS 12:26 pm Boletín Fiscal Aduanero, NANO Fit Importadores y Exportadores

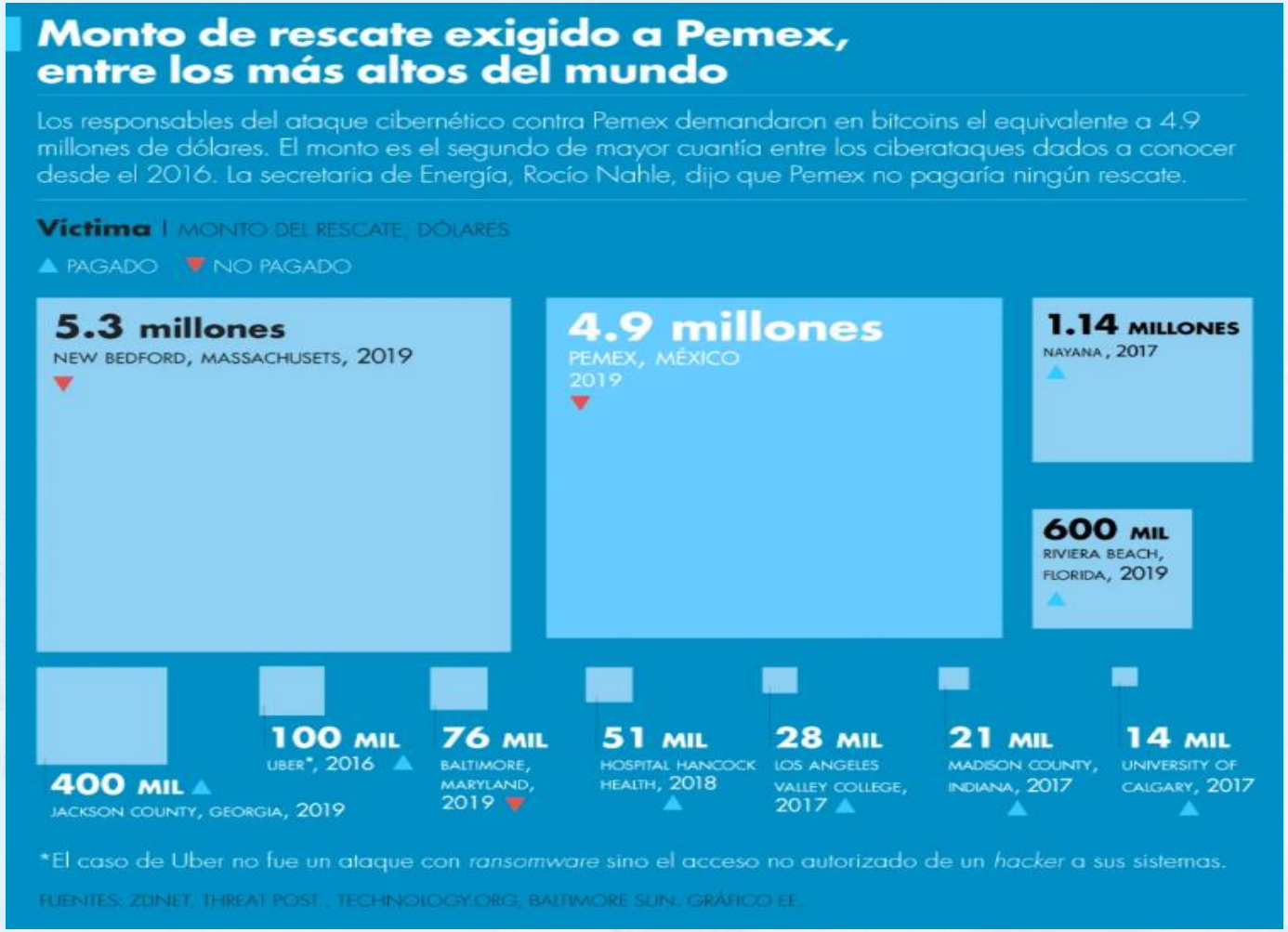
En enero 2021, Customs and Border Protection (CBP) emitió a través del portal de C-TPAT el boletín "Ciberamenazas: La Nube y Conexiones Remotas", en el cual informa a los miembros de C-TPAT la importancia de la ciberseguridad, así como de las distintas amenazas a las que pueden ser susceptible al trabajar de forma remota y utilizar la nube para realizar actividades empresariales.

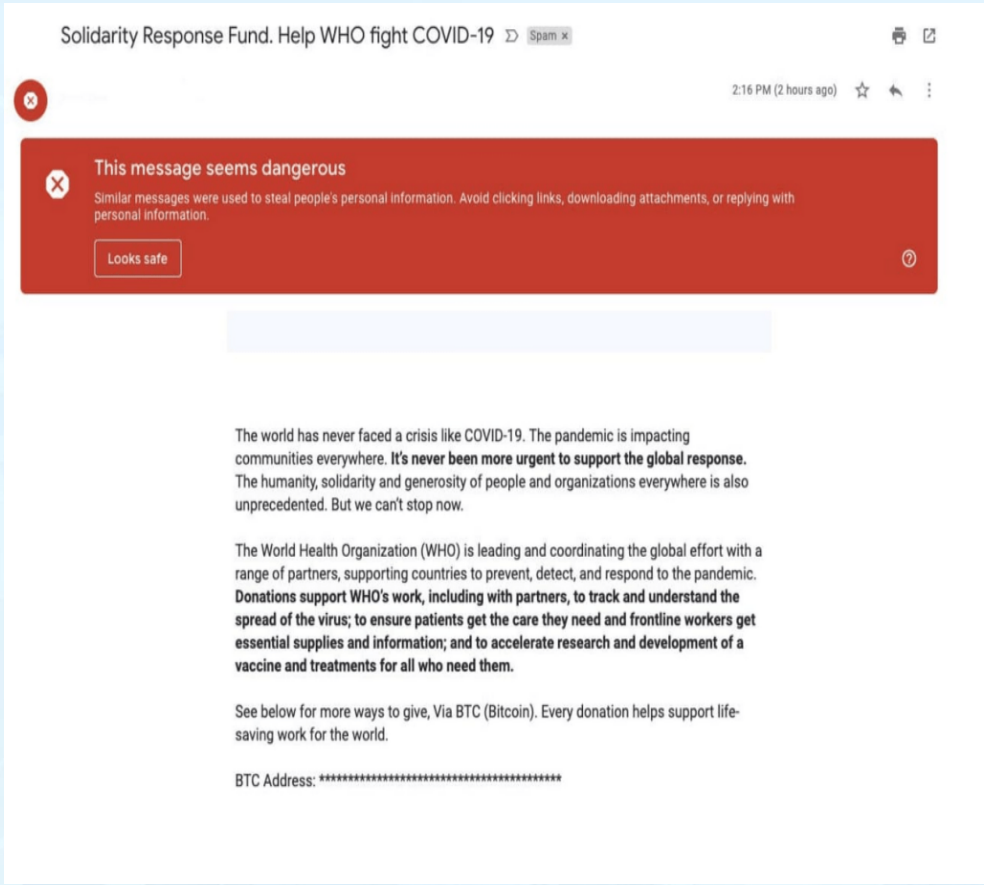
Debido a la contingencia sanitaria que está afectando al mundo en estos momentos, muchos de los miembros C-TPAT decidieron

In January 2021, Customs and Border Protection (CBP) issued through the C-TPAT portal the newsletter "Cyber Threats: The Cloud and Remote Connections", which informs C-TPAT members of the importance of cybersecurity, as well as the several threats they may be susceptible to when working remotely and using the cloud to conduct business.

Due to the health contingency that is affecting the world right now, many C-TPAT members decided to work remotely or in remote work

https://www.tlcasociados.com.mx/alerta-c-tpat-por-ciberamenazas-en-teletrabajo/





https://phishingquiz.withgoogle.com/?hl=es
https://www.interbel.es/phishing-2022/

Ciberseguridad

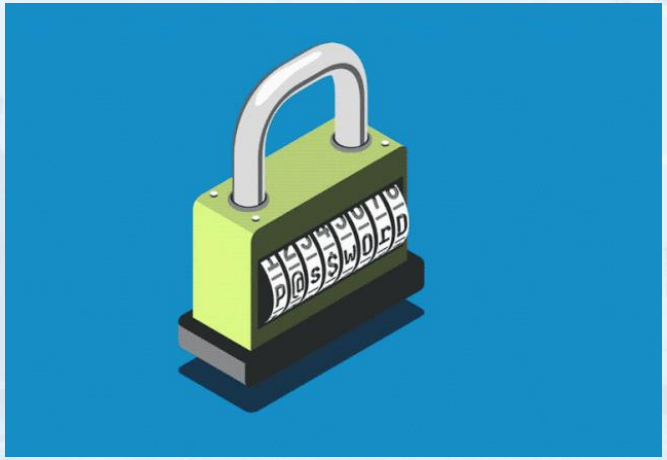
Las políticas y los procedimientos de ciberseguridad se deben **revisar anualmente**, o con mayor frecuencia, según lo establezcan el riesgo o las circunstancias. Después de la revisión, las políticas y los procedimientos se deben actualizar, en caso de ser necesario.

El *acceso del usuario* debe restringirse según la *descripción del trabajo* o las tareas asignadas. El acceso autorizado se debe revisar periódicamente para garantizar que el acceso a sistemas sensibles se base en los requisitos del trabajo. El acceso a las computadoras y la red debe eliminarse tras la separación del empleado de la empresa.

Ciberseguridad

Las personas con acceso a los sistemas de Tecnología de la Información (TI) deben usar cuentas asignadas individualmente. El acceso a los sistemas de TI debe protegerse de la infiltración mediante el uso de **contraseñas fuertes, frases secretas u otras formas de autenticación**, y el acceso del usuario a los sistemas de TI debe estar protegido. Las contraseñas o frases secretas se deben cambiar tan pronto sea posible si existen indicios o sospecha razonable de que están comprometidas.

Para proteger los sistemas de TI de infiltraciones, se debe proteger el acceso del usuario mediante un proceso de autenticación. Las contraseñas o frases de acceso complejas para iniciar sesión, las tecnologías biométricas y las tarjetas de identificación electrónicas son tres tipos diferentes de procesos de autenticación.



Ciberseguridad

-Cambiarse mínimo cada 90 días

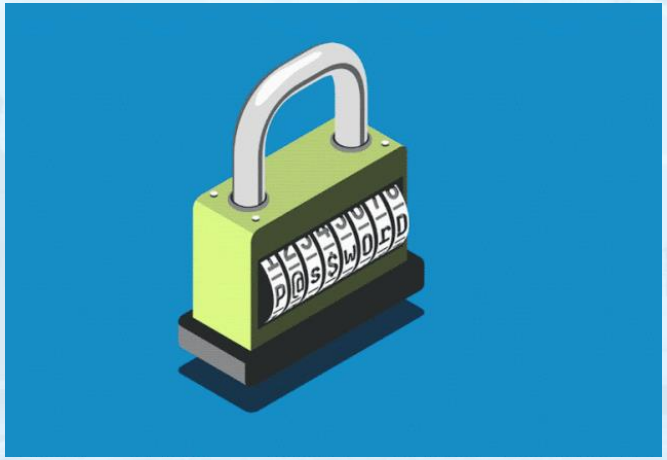
-Evitar usar nombre del personal/empresa/puesto (Clip123, Esmeralda456, etc)

-Evitar usar series numéricas

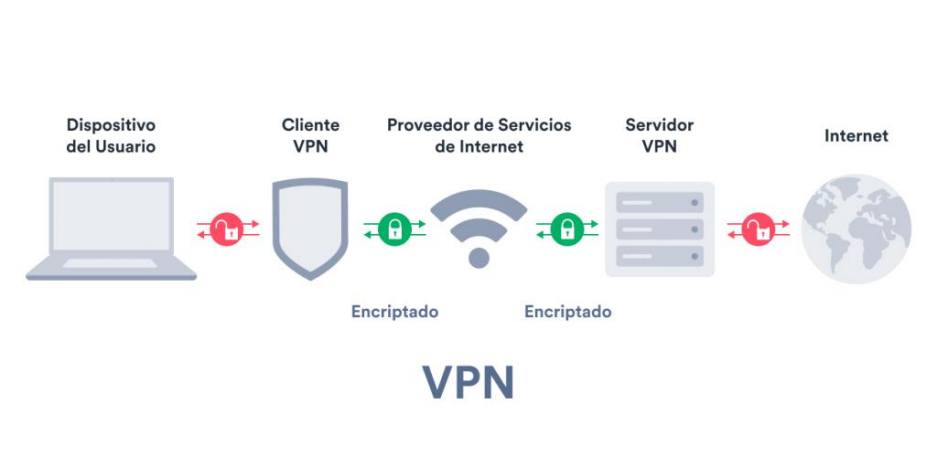
-Evitar usar indicios muy fáciles de adivinar

-Utilizar varios caracteres y distintos tipos (/*-+)

https://ciberprotector.com/comprobador-de-contrase%C3%B1as/



Ciberseguridad



Las **VPN** no son la única opción para proteger el acceso remoto a una red. La autenticación multifactor (MFA) es otro método. Un ejemplo de autenticación multifactor sería un token con un código de seguridad dinámico que el empleado debe ingresar para acceder a la red.

Los miembros que permiten que sus **usuarios se conecten de forma remota** a una red deben emplear tecnologías seguras, como redes privadas virtuales (VPN) para permitir que los empleados accedan a la intranet de la empresa de forma segura cuando se encuentran fuera de la oficina. *Los miembros también deben tener procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados.*

Ciberseguridad

Si los miembros permiten que los empleados utilicen dispositivos personales para realizar el trabajo de la empresa, todos esos dispositivos *deben cumplir con las políticas y procedimientos de seguridad cibernética de la empresa* con respecto a incluir actualizaciones de seguridad periódicas y un método para acceder de manera segura a la red de la empresa.

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.*

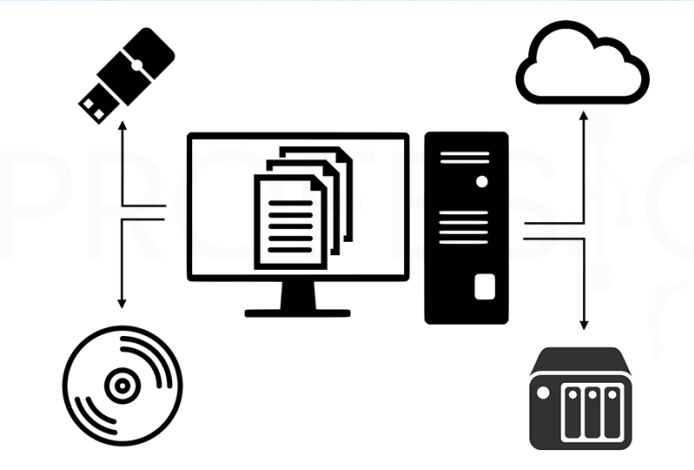
Ciberseguridad

Las políticas y los procedimientos de seguridad cibernética deberían incluir medidas para **evitar el uso de productos tecnológicos falsificados o con licencias inapropiadas.**

El software sin licencia tiene más probabilidades de **fallar** dada la imposibilidad de actualizarlo. Es más propenso a contener **programas malignos**, los cuales dejan inservibles las computadoras y la información que estas contengan. No se debe esperar garantías ni respaldo técnico para el software que no tiene licencia, lo cual significa que la empresa debe hacerle frente a cualquier falla por su propia cuenta. También hay **consecuencias legales** para el software sin licencia, incluidas las penas civiles severas y el procesamiento penal. Los piratas de software aumentan los costos para los usuarios del software legítimo y autorizado y disminuyen el capital disponible para invertir en investigación y desarrollo de nuevo software. *Sería recomendable que los miembros tengan una política que requiera conservar las etiquetas de la clave de producto y los certificados de autenticidad cuando se compren medios informáticos nuevos*.

Ciberseguridad

Se debería realizar una **copia de seguridad** de los datos una vez por semana o según sea apropiado. Todos los datos confidenciales y sensibles se deberían almacenar en formato cifrado.



También se recomienda realizar copias de seguridad diarias en caso de que los servidores compartidos o de producción se vean comprometidos o pierdan datos. Los sistemas individuales pueden requerir respaldos menos frecuentes, dependiendo del tipo de información con la que se está trabajando. *Los medios utilizados para guardar los respaldos de seguridad deberían guardarse preferiblemente en un lugar fuera de las instalaciones*. Los dispositivos utilizados para respaldar los datos no deberían estar en la misma red que la utilizada para el trabajo de producción. El respaldo de los datos en la nube es aceptable como un lugar “fuera de las instalaciones”.

Ciberseguridad

Todos los medios, hardware u otro equipo de TI que contengan información sensible respecto al proceso de importación y exportación deben **contabilizarse mediante la realización periódica de inventarios**. Cuando se descarten, se deben vaciar o destruir adecuadamente de acuerdo con las Directrices del Instituto Nacional de Normas y Tecnología (NIST) para la Limpieza de Medios u otras directrices de la industria apropiadas.

Algunos tipos de medios informáticos son los discos duros, las unidades extraíbles, los discos CDROM o CD-R, DVD o las unidades USB. El Instituto Nacional de Normas y Tecnología (NIST) ha desarrollado las normas de destrucción de medios de datos del gobierno. Se aconseja a los miembros consultar las normas del NIST para limpiar y destruir equipos y medios informáticos.

NIST

- Instituto Nacional de Estándares y Tecnlogía
- Fue fundado en 1901, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica.

9 Seguridad de la información y documentación

Deben existir **medidas de prevención** para *mantener la confidencialidad e integridad de la información y documentación* generada por los sistemas de la empresa, incluyendo aquellos utilizados para el intercambio de información con otros integrantes de la cadena de suministros. Asimismo, deben existir políticas documentadas que incluyan las medidas contra su mal uso.

9.1 Clasificación y manejo de documentos

oea Operador Económico Autorizado MÉXICO

Deben existir procedimientos para clasificar documentos de acuerdo a su sensibilidad y/o importancia. La documentación sensible e importante debe ser almacenada en un área segura que solamente permita el acceso a personal autorizado. Se debe identificar el tiempo de vida útil de la documentación y establecer procedimientos para su destrucción.

La empresa deberá conducir revisiones de forma regular para verificar los accesos a la información y asegurarse de que no sean utilizados de manera indebida.

Procedimiento documentado para el registro, control y almacenamiento de documentación impresa (clasificación y archivo de documentos).

-Registro de control para entrega, prestamos, entre otros de documentación
-Acceso restringido al área de archivos
-Políticas de almacenamiento

Plan de seguridad actualizado que describa las medidas en vigor relativas a la protección de los documentos contra accesos no autorizados, así como contra la destrucción deliberada o a la perdida de los mismos

9.2 Seguridad de la Tecnología de la Información

oea Operador Económico Autorizado MÉXICO

En el caso de los sistemas automatizados, se deben utilizar cuentas individuales que exijan un cambio periódico de la contraseña. Debe haber políticas, procedimientos y normas de tecnología de informática establecidas que se deben comunicar a los empleados mediante capacitación.

Deben existir procedimientos escritos e infraestructura para proteger a la empresa **contra pérdidas, robo, fuga, hackeo y/o secuestro de información**, así como un sistema o software establecido para *identificar el abuso de los sistemas de tecnología de la información y detectar el acceso inapropiado y/o la manipulación indebida o alteración* de los datos comerciales y del negocio, así como un procedimiento escrito para la aplicación de medidas disciplinarias apropiadas a todos los infractores

9.2 Seguridad de la Tecnología de la Información

oea Operador Económico Autorizado MÉXICO

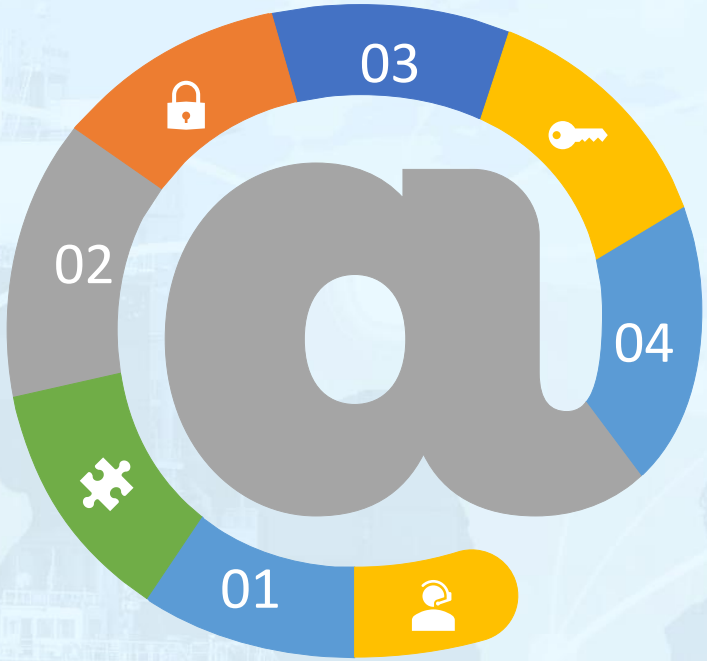
Señale la frecuencia con que se llevan a cabo las copias de respaldo de la información

Quién tiene acceso a los mismos y quién autoriza la recuperación de la información.

Describa el procedimiento para la protección de sus sistemas informáticos y como garantizan la seguridad de la informació

Indique si los sistemas están protegidos bajo contraseñas y con qué frecuencia son modificadas.

Señale si existen políticas de seguridad de la información para su protección.



Indique los mecanismos o sistemas para detectar el abuso o intrusión de personas no autorizadas a sus sistemas.

Indique las políticas correctivas y/o sanciones en caso de la detección de alguna violación a las políticas de seguridad de la información.

Señale si los socios comerciales tienen acceso a los sistemas informáticos de la empresa. En su caso, indique qué programas y cómo controlan el acceso a los mismos

Indique si el equipo de cómputo cuenta con un sistema de respaldo de suministro eléctrico que permita la continuidad del negocio.

Seguridad de la Tecnología de la Información

Quién es responsable de la protección del sistema informático de la empresa

Detallar si opera con sistemas múltiples (sedes/sitios) y cómo se controlan dichos sistemas

Una política actualizada y documentada de protección de los sistemas informáticos de la empresa de accesos no autorizados y destrucción deliberada o pérdida de la información.

Pruebas de la validez de la recuperación de los datos a partir de copias de seguridad.

Cómo y por cuánto tiempo se almacenan los datos

Plan de continuidad del negocio en caso de incidente y de cómo recuperar la información

Frecuencia y localización de las copias de seguridad y de la información archivada

Si las copias de seguridad se almacenan en sitios alternativos a las instalaciones donde se encuentra el CPD (centro de proceso de datos).

Seguridad de la Tecnología de la Información

oea Operador Económico Autorizado MÉXICO

Medidas previstas para tratar incidentes en caso de que el sistema se vea comprometido

Cómo se conceden autorizaciones de acceso y nivel de acceso al sistema informático (el acceso a la información sensible debe estar limitado al personal autorizado a realizar modificaciones información).

Formato de las contraseñas, frecuencia de cambios y quién proporciona esas contraseñas.

Eliminación, mantenimiento o actualización de los detalles de usuario.

Nombre del cortafuegos "firewall" y anti-virus utilizados (incluir lo relacionado al licenciamiento).

CUEJ
CENTRO UNIVERSITARIO DE ESTUDIOS JURÍDICOS
PLANTEL BAJA CALIFORNIA

TLC ASOCIADOS

TRADE LAW & CUSTOMS magazine

Trade & Law College

DIPLOMADO EN CERTIFICACIONES DE SEGURIDAD DE LA CADENA DE SUMINISTROS

A 10 años de la implementación de OEA en México.

Contáctanos: **desarrollo.academico@tradelawcollege.edu.mx** Tel. (664) 200 2770 Cel. (663) 167 2862 **www.tradelawcollege.edu.mx**