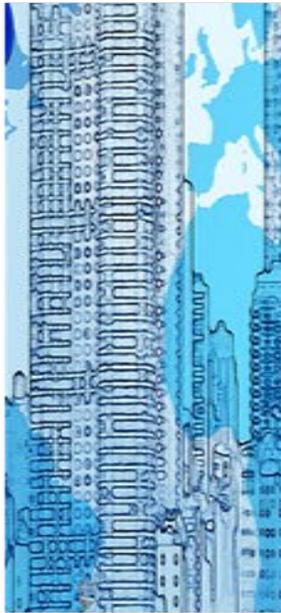
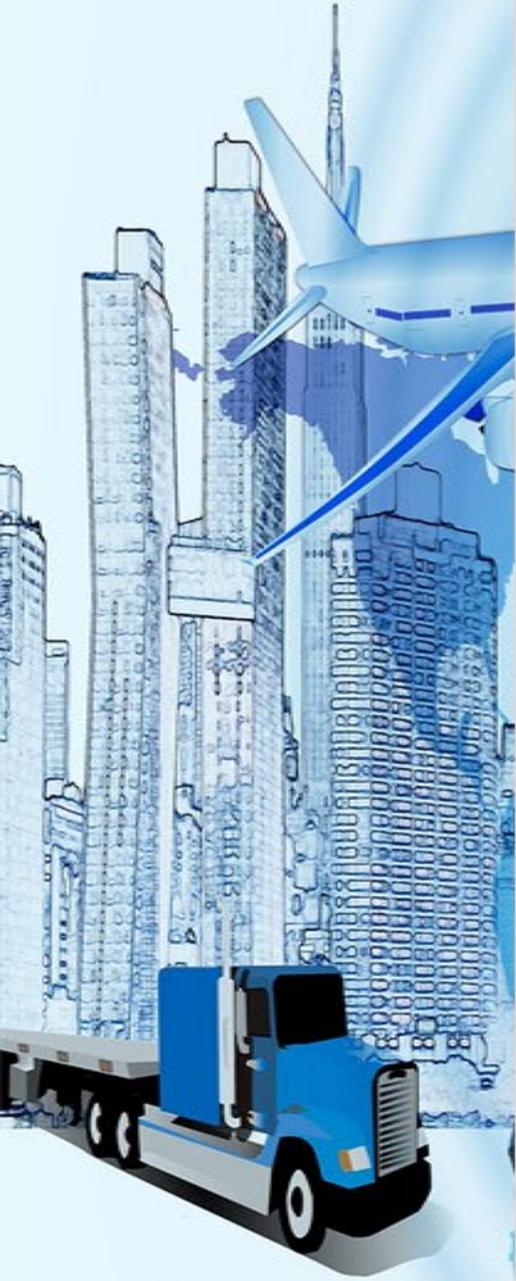


PERFIL DE SEGURIDAD SECTOR EXPORTADOR/IMPORTADOR
POLÍTICAS DE GESTIÓN Y CRITERIOS MÍNIMOS DE SEGURIDAD



PERFIL DE SEGURIDAD OEA
SECTOR EXPORTADOR/IMPORTADOR
POLÍTICAS DE GESTIÓN Y CRITERIOS MÍNIMOS DE SEGURIDAD

I. ALCANCE

El presente documento tiene por finalidad establecer el conjunto de políticas de gestión y criterios mínimos de seguridad que deben observar las personas naturales o jurídicas en el desarrollo de sus actividades y operaciones comerciales reguladas por la Autoridad Aduanera, a efectos de lograr el cumplimiento de los requisitos para optar por la condición de Operador Económico Autorizado Honduras (OEA).

II. POLÍTICAS DE GESTIÓN PARA EL CONTROL Y SEGURIDAD DE LAS OPERACIONES COMERCIALES**1. Voluntariedad**

El Exportador/Importador que voluntariamente se someta al proceso de habilitación como OEA, asume los compromisos y obligaciones que sobre el particular disponga el Servicio Aduanero y se deriven de la concesión de OEA en el país.

2. Seguridad

El Exportador/Importador debe perfeccionar e incorporar mejores prácticas de seguridad y bioseguridad en sus operaciones comerciales y aduaneras, en conjunto con la Administración aduanera.

3. Control Interno

El Exportador/Importador debe efectuar una validación inicial de su situación actual en materia de procedimientos y medidas de seguridad, incorporando en sus procesos:

- *Valoración de riesgo:* Mediante la identificación, análisis, evaluación y corrección de las malas prácticas.
- *Auditoría Periódica:* Evaluar todos los procesos y medidas de seguridad de acuerdo con el modelo de negocio.

4. Medios Tecnológicos

El Exportador/Importador debe incorporar dentro de sus procesos el uso voluntario de tecnologías más avanzadas, con el fin de asegurar los controles y medidas de seguridad que se apliquen en sus operaciones.

5. Comunicación

El Exportador/Importador debe mantener una comunicación directa sobre las medidas de seguridad utilizadas, con las partes implicadas en la cadena logística, así como una coordinación con la Autoridad Aduanera sobre los aspectos operativos, con el fin de analizar aquellos que sean de interés mutuo (normativa aduanera, procedimientos y

requisitos de seguridad y bioseguridad) que sirvan para el intercambio de información y mejora de los procesos aplicados.

6. Facilitación

El Exportador/Importador que ostente la condición de OEA, debe poner disposición de la Autoridad aduanera la información necesaria, a fin de facilitar las evaluaciones que sobre sus sistemas de gestión, logística y seguridad deban efectuarse por las mismas.

7. Formación y sensibilización del personal

De acuerdo con el modelo comercial la empresa, debe desarrollar medidas y programas de seguridad para promover la integridad de los procedimientos respecto al transporte, mantenimiento y almacenamiento de carga en la cadena logística protegida.

La empresa debe proporcionar capacitación específica para ayudar a los empleados a garantizar la integridad de la carga, reconocer posibles amenazas internas de seguridad y controlar el acceso. La empresa debe informar a los empleados de los procedimientos aplicados por la empresa para identificar y señalar incidentes sospechosos.

III. PLANEACIÓN DE LA SEGURIDAD EN LA CADENA LOGÍSTICA

El Operador Económico debe contar con una metodología que le permita identificar, analizar y adoptar las medidas necesarias para minimizar y dar seguimientos a los riesgos que pueden afectar su operativa comercial, entre los temas a considerar:

1. **Análisis de riesgo.** Debe identificar las áreas de mayor impacto y de oportunidad para implementar mecanismos que le permitan mantener la integridad de sus mercancías.
2. **Plan de contingencias y/o emergencias.** Debe asegurar la continuidad del negocio en el caso de una situación que afecte el desarrollo normal de las actividades y las operaciones de comercio exterior del Operador Económico en su cadena logística.
3. **Revisión gerencial.** La alta Dirección debe estar siempre involucrada en la revisión y supervisión de los procesos en su cadena logística, y de esta forma se adoptará la cultura de seguridad en todos los niveles de la empresa.
4. **Auditoría interna en la cadena logística.** Se debe contar con un procedimiento de revisión interna, que se asegure se cumplen los procesos en cada una de las áreas en materia de seguridad en la cadena logística.
5. **Registro de incidencias.** El operador debe contar con un registro de incidencias que ayude a identificar las áreas o procesos que por alguna situación hayan sido vulnerados y que correspondan a la cadena logística. Además de establecer el tratamiento que se le dio a la situación en su momento para tomar las medidas correctivas pertinentes y evitar que vuelvan a ocurrir.

IV. CRITERIOS MÍNIMOS DE GESTIÓN Y SEGURIDAD.

Los criterios mínimos de gestión y seguridad se refieren a los aspectos que debe considerar el solicitante para la obtención de la habilitación como OEA en el país, los mismos responden a prácticas comerciales y medidas de control que deben observar durante sus

operaciones de logística, seguridad e interrelación con los socios comerciales y su cadena logística. Estos comprenden el desarrollo de tres secciones diferentes que contemplan los requisitos del Programa OEA

Sección 1: Procesos Administrativos

- A. Antecedentes de Cumplimiento Administrativo, Aduanero, Tributario y Judicial.
- B. Gestión Administrativa, Contable y de Logística adecuada.
- C. Solvencia Financiera Acreditada.

Sección 2: Administración de Recurso Humano**Sección 3: Medidas en Materia de Protección y Seguridad****SECCION 1: PROCESOS ADMINISTRATIVOS****A. Historial Satisfactorio de Cumplimiento Administrativo, Aduanero, Tributario y Judicial.**

Constituye un historial satisfactorio que el solicitante debe cumplir de conformidad con el ordenamiento jurídico, tributario y aduanero vigente, a fin de obtener la condición de Operador Económico Autorizado en Honduras (OEA).

1. El solicitante debe disponer y actualizar los permisos o autorizaciones requeridos para una correcta ejecución de sus actividades comerciales.
2. El solicitante debe encontrarse al día con el pago de sus obligaciones aduaneras y tributarias, en relación con la presentación de declaraciones, pago de impuestos, tasas y multas. Además, de no haber sido objeto de auditorías y ajustes en las áreas Tributaria y Aduanera, dentro de los tres años anteriores a la presentación de su solicitud de habilitación como OEA.
3. El solicitante debe cumplir con lo establecido en el Código Tributario, en el decreto 170-2016 en el Título Sexto de las Infracciones Tributarias, Ley de Impuesto Sobre la Renta Capítulo X, y el Reglamento de la Ley de Impuesto sobre la Renta Título XI Capítulo 2° y 3° y Título XIII.
4. El solicitante, el Representante Legal, Consejo de Administración, Junta Directiva u Órganos de Dirección, deben estar libres de sentencias en los tres años anteriores a la presentación de la solicitud, en delitos penales; los contemplados en nuestro Código Penal, en el Título V Delitos contra la salud Pública, Título VII Delitos contra la Propiedad, Título IX Delitos contra la Fe Pública, Capítulo XI Delitos contra la existencia y seguridad del Estado, Título XIII Delitos contra la Administración Pública.
5. Las constituidas en el Artículo 28, Título VIII, Capítulo I de las Infracciones Aduaneras y sus Sanciones, Capítulo II de las reclamaciones y los recursos aduaneros estipulados en el Código Aduanero Uniforme Centroamericano (CAUCA IV), Resolución 368-2015 (COMIECO LXXIII) modificaciones de la Sección XIII del Capítulo VII del Título II Artículos 159 al 166 del RECAUCA IV.

B. Gestión Administrativa, Contable y de Logística Adecuada.

La autoridad aduanera validará las formalidades seguidas por el exportador/importador para llevar a cabo las operaciones aduaneras y prácticas comerciales, por lo que debe cumplir lo siguiente:

B.1 Gestión Administrativa:

1. El solicitante debe poseer un sistema o metodología de control interno que permita efectuar una valoración de riesgo sobre las operaciones aduaneras y comerciales realizadas, para ello requiere:
 - Identificar los riesgos relevantes asociados al logro de los objetivos y metas propuestas de la empresa.
 - Analizar el posible efecto de los riesgos identificados en la empresa, importancia y probabilidad de que ocurran.
 - Adoptar medidas necesarias para administrar o establecer los mecanismos operativos que minimicen las acciones riesgosas.
 - Comprobación y seguimiento de las medidas adoptadas sobre los riesgos detectados.
2. El solicitante debe efectuar comprobaciones y evaluaciones de las políticas internas, procedimientos y medidas de seguridad sobre sus operaciones.
3. El solicitante debe disponer de un procedimiento documentado que permita llevar el control sobre el registro y modificación de los datos generales de los proveedores, clientes y productos que se comercializan para la importación y exportación.

B.2 Sistema de Contabilidad:

El solicitante debe utilizar un sistema contable generado mediante un sistema informático para el control del giro de su negocio, así como de sus operaciones aduaneras y comerciales en las que se considere:

- Tipo de sistema contable utilizado y periodo de actualizaciones.
- Personal responsable del mantenimiento y actualización del sistema contable.

B.3 Logística Adecuada:

1. El solicitante debe disponer de un procedimiento que especifique las acciones a seguir para la atención y presentación de los trámites aduaneros, declaraciones aduaneras y documentos adjuntos, en el que se incluya:
 - Formalidades seguidas para asegurar una correcta elaboración y transmisión de las declaraciones aduaneras.
 - Formalidades exigidas para la comunicación por parte de la empresa al agente aduanero, sobre instrucciones o errores en las operaciones y trámites realizados.
 - Criterios para el control y seguimiento de las actividades u operaciones aduaneras que realiza el agente aduanero en nombre de la empresa.

2. Cuando corresponda, la empresa interesada debe disponer de un registro actualizado, sobre las mercancías que se encuentren sujetas a:
 - Licencias asociadas a políticas comerciales y políticas agrícolas.
 - Permisos, certificados o restricciones.
3. Debe tener definida una política de firma y sellos que autoricen los diferentes procesos.

C. Solvencia Financiera Acreditada.

La administración aduanera validará que el exportador/importador durante los tres años anteriores a la presentación de la solicitud, ha demostrado un adecuado cumplimiento y capacidad de pago de sus compromisos adquiridos y que cuenta con los bienes y recursos suficientes para hacer frente a tales obligaciones.

Aspectos de solvencia:

1. Debe mantener actualizados sus estados financieros.
2. Debe realizar dentro del año fiscal, al menos una auditoría interna o externa sobre sus estados financieros
3. No debe encontrarse en un proceso de acreedores, ser declarado judicialmente en quiebra o insolvencia, o en procesos de administración y reorganización con intervención Judicial.

SECCIÓN 2: ADMINISTRACIÓN DEL RECURSO HUMANO

Es importante contar con políticas de contratación de personal (permanente y temporal) con base en el análisis de riesgo. Las responsabilidades se deben definir antes de la contratación laboral mediante la descripción adecuada del trabajo, términos y condiciones del empleo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deben seleccionar adecuadamente, especialmente para los trabajos en áreas críticas.

Asegúrese que se emplea un proceso de validación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deben firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

1. Debe tener un procedimiento documentado para la selección y contratación del personal (permanente y temporal), que incluya una validación de la información de la solicitud de empleo, análisis de los antecedentes, estudio socioeconómico y visitas domiciliarias.
2. Debe realizar pruebas para detectar consumo de alcohol, drogas y otras adicciones al personal de áreas críticas, antes de la contratación, aleatoriamente y cuando exista una sospecha justificable.
3. Debe disponer de un expediente actualizado de cada uno de los empleados, que incluya como mínimo información personal y familiar, fotografía, registro de huella dactilar y firma.

4. Debe tener un programa que proporcione a sus empleados inducción y capacitación permanente sobre las políticas y procedimientos de seguridad física, personal, de la carga y del transporte, manejo de equipo de seguridad e higiene industrial, de la tecnología informática, así como las implicaciones por incumplimiento de las mismas.
5. El personal con responsabilidades de seguridad debe recibir capacitación permanente que cubre entre otros: el mantenimiento de la integridad de la carga, accesos no autorizados, fraudes en documentos, sistemas de información, prácticas anti-contrabando y antiterroristas.
6. Debe tener un procedimiento documentado que indique como reportar y dar seguimiento a las actividades consideradas sospechosas, que muestren señales de conspiraciones internas, consumo de drogas ilícitas y todas aquellas que representen un riesgo para la seguridad de la empresa.
7. Debe tener definidas disposiciones de seguridad adecuados para el suministro y manejo del carné y uniformes, que incluya el control de entrega, devolución o cambio de estos.
8. Debe tener definidas las cláusulas de confidencialidad y responsabilidad en los contratos del personal en áreas críticas.
9. El personal debe contar con un dispositivo de identificación (carnés, tarjetas de acceso, camisas etc.).
10. Debe llevar control y registro de las capacitaciones impartidas a cada uno de sus empleados.
11. Debe tener definido un reglamento que establezca medidas disciplinarias y/o sanciones a aplicar por faltas cometidas.
12. Debe tener procedimientos documentados que indiquen la forma de proceder cuando el personal se retire definitivamente de la empresa.
13. Debe tener definidas responsabilidades y obligaciones a la hora de finalizar la relación laboral o al realizar un cambio de puesto del personal.

SECCIÓN 3: MEDIDAS EN MATERIA DE PROTECCIÓN Y SEGURIDAD.

A. Medidas en materia de protección y seguridad.

Constituye medidas o niveles de seguridad que deben estar presentes en todas las áreas e instalaciones, controles de acceso, medidas de manipulación de las cargas y transporte, aspectos sobre la identificación de los socios comerciales y empleados.

B. Asociados de negocios (Clientes/Proveedores)

Los Asociados de Negocio deben estar comprometidos a trabajar por la misma causa de seguridad de la cadena logística. Con esto, se debe asegurar que su Sistema de Gestión de Riesgos este apoyado para poder confiar que se tomarán las medidas necesarias y pertinentes, que permitan garantizar la entrega del producto o prestación del servicio, el cual, será controlado de tal forma que se evite cometer cualquier acto ilícito por intermedio suyo, convirtiéndose así en aliados para garantizar una cadena de comercio segura, libres de todo tipo de acto ilícito, tales como nexos con grupos alzados en armas, terroristas, narcotráfico, lavado de activos etc.

Sus asociados de negocio deben garantizar que su personal es calificado, idóneo y ha sido previamente capacitado para desempeñar las funciones de su actividad comercial, además de ser seleccionado adecuadamente mediante un estricto proceso, cuyo registro muestre: hoja de vida, cédula de identidad, afiliación al seguro social, certificado de antecedentes judiciales y policiales, además de las referencias personales, entre otros. Sera su responsabilidad validar la credibilidad y confiabilidad de sus asociados de negocio.

1. Debe existir procedimientos documentados para la selección, evaluación y conocimiento de sus asociados de negocio (clientes/proveedores) que garanticen su confiabilidad
2. Debe contar con acuerdos para socios comerciales que permitan garantizar la inclusión de medidas de seguridad en la cadena logística
3. Debe contar con procedimiento para comprobar que los socios comerciales cumplan con las cláusulas de seguridad de la cadena logística
4. Basado en un proceso de análisis y evaluación de riesgos, debe realizar y documentar una visita anual a las instalaciones donde sus asociados de negocio desarrollen sus operaciones, con el fin de validar si éstos cumplen los criterios mínimos de seguridad.
5. Debe Mantener un registro actualizado con la información de sus socios comerciales
6. En los casos que transfiera, delegue, tercerice o subcontrate alguno de sus recursos o procesos relacionados con su cadena logística, el prestador del servicio u outsourcing debe garantizar que cumple los requisitos mínimos de seguridad.
7. Debe reportar a la autoridad competente la identificación de actividades sospechosas, en caso de que se presenten.

C. Control de Acceso

Un control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas denominadas protegidas (o áreas críticas). En una empresa o comercio los elementos a proteger pueden ser fácilmente identificables, como las zonas donde se manipula dinero, donde se guardan los registros del personal y planos de sus productos (propiedad intelectual), entre otras, y algunas no tan obvias, como los sectores del proceso productivo con técnicas de fabricación consideradas únicas o propias.

En otras ocasiones es necesario proteger áreas donde solo puede haber personal técnicamente capacitado como salas de energía, desechos peligrosos, etc. O, simplemente, el control de accesos también puede ser utilizado para mantener a los obreros/empleados en las áreas donde realizan sus tareas, evitando así personas deambulando por sectores donde no deberían estar para no perturbar el normal funcionamiento de la empresa.

Por tanto, siempre que se coloque un control de accesos, debe considerarse que éste divide el espacio general en dos o más subáreas, una denominada externa o sin protección o de acceso general y otras internas, denominadas protegidas o de accesos restringidos.

1. Debe tener un procedimiento documentado de identificación de empleados para controlar el acceso a la empresa y áreas donde desempeñan sus funciones.
2. Debe tener procedimientos documentado para la entrega, devolución y cambio de dispositivo de acceso como carnés de identificación, tarjetas u otra para los empleados.
3. Debe tener procedimiento documentado procedimiento documentado que regule el registro y control del personal de la empresa, personal subcontratado, visitantes, proveedores, contratistas, vendedores, agencias de correo y vehículos que ingresan a las instalaciones.
4. Debe tener documentados procedimientos de control para los medios de transporte y mercancías que entren, salgan o permanezcan en las instalaciones de la empresa, que incluya como validar la información de los documentos donde se registra el ingreso, almacenaje, manipulación, entrega, pesaje, recuento y control de la mercancía y el marchamo cuando corresponda.
5. Debe tener procedimientos documentados que establezcan la actuación a seguir por parte del personal ante el descubrimiento de cualquier circunstancia fuera de la operación normal.
6. Debe tener un procedimiento documentado para identificar y dirigirse a personas no autorizadas o no identificadas conforme la circunstancia.
7. Debe contar con un procedimiento documentado que defina el acceso a las diferentes áreas de la empresa, haciendo distinción de las regulaciones aplicables para los accesos a áreas con acceso restringido.
8. Debe tener un procedimiento para el manejo de llaves, cerrojos y dispositivos de cierre.

D. Seguridad Física en las Instalaciones:

La seguridad física se refiere a la identificación y análisis de las amenazas y riesgos que enfrentan o pueden llegar a enfrentar instalaciones, bienes y procesos a fin de implementar planes y sistemas tendientes a prevenir, dificultar o limitar los resultados de las posibles acciones dañinas contra la seguridad de la empresa.

Las medidas de seguridad física aplicables deben tender a: impedir la entrada por parte de intrusos, disuadir, impedir o detectar acciones llevadas a cabo por personal desleal, limitar al personal en su acceso a información clasificada, detectar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones de corrección sobre éstas a la mayor brevedad posible.

1. Debe tener definidas políticas de seguridad física de las instalaciones.
2. Debe definir áreas consideradas críticas en sus instalaciones.
3. Debe tener designado un responsable que garantice el control de las llaves de acceso a las diferentes áreas.
4. Debe contar con cercas, barreras o muros perimetrales alrededor de sus instalaciones y de las áreas de manejo y almacenamiento de carga.

5. Debe tener aseguradas las puertas, ventanas, cercas y barreras interiores y exteriores.
6. Debe contar un procedimiento documentado para inspección de cercas, barreras perimetrales, puertas, ventanas que permita validar la integridad e identificar daños, en el cual se incluya como registrar los hallazgos.
7. Las puertas de ingreso y salida de vehículos y personal deben estar controladas, monitoreadas y supervisadas.
8. Debe prohibir el estacionamiento de vehículos en áreas de manejo y almacenamiento de carga o adyacentes a la entrada y salida de las mismas.
9. Debe disponer de señalización e iluminación adecuada dentro y fuera de las instalaciones.
10. Las instalaciones deben estar construidas con materiales que resistan la entrada forzada o ilegal.
11. Debe realizar inspecciones y reparaciones periódicas para mantener la integridad de las instalaciones.
12. Debe utilizar sistemas de alarma, cámaras de vigilancia monitoreada para alertar, registrar, supervisar las instalaciones y prevenir el acceso no autorizado a las áreas críticas.
13. Debe tener un servicio de vigilancia y seguridad que garantice una acción de respuesta oportuna y disponibilidad las 24 horas del día, en su caso.
14. Debe tener un programa de mantenimiento preventivo y correctivo de los dispositivos de seguridad física (cámaras, sistema de alarma, inspecciones de cerca, guardia de seguridad, etc).
15. Debe separar y controlar las áreas destinadas a casilleros, vestidores y similares de las áreas críticas de la empresa.
16. Debe tener designado un responsable de la seguridad general de toda la empresa, que coordina y supervisa la actuación del personal ante el descubrimiento de cualquier circunstancia fuera de la operación normal.

E. Medidas de Bioseguridad

En el marco de las medidas necesarias para prevenir la propagación del coronavirus (COVID-19), y salvaguardar el derecho a la vida y proteger la salud de los ciudadanos en general, se requiere el cumplimiento de las siguientes medidas para todo el que visite o permanezca en las instalaciones físicas de la empresa:

E1. Medidas generales

1. Debe crear y mantener una política de bioseguridad que contenga los protocolos y procedimientos a seguir de prevención y atención de sospechosos.
2. Debe establecer controles de ingeniería y controles administrativos para garantizar el distanciamiento seguro de 1.5 a 2 metros entre los colaboradores en los diferentes puestos de trabajo, áreas y departamentos.

3. Debe realizar un análisis de riesgo que le permita identificar al personal vulnerable debido a edad o condiciones clínicas de padecimientos y proceder al aislamiento y solo convocarles en condiciones de extrema necesidad.
4. Debe colocar dosificadores de desinfectante de manos en lugares visibles en el lugar de trabajo, asegurándose de que los dosificadores se recargan frecuentemente.
5. Debe elaborar un plan de emergencia y de continuidad de las actividades de la empresa en caso de que se declare un brote en las comunidades donde opera su empresa.

E2. Obligaciones

1. Debe fumigar con sustancias sanitizantes los vehículos previos al ingreso al estacionamiento de las instalaciones, toma de temperaturas y aplicar medidas de desinfección para la ropa, manos y zapatos en las entradas del establecimiento.
2. Debe colocar dispositivos de contención o cualquier otro mecanismo en las secciones donde se deba tener contacto directo con clientes externos.
3. Debe proporcionar al personal los elementos de bioseguridad necesarios y adecuados, según el puesto de trabajo (protección de ojos, nariz, boca, manos, piel, pies y calzado)
 - Protección ocular (gafas, lentes, espejuelos, caretas).
 - Boca (mascarilla, tapaboca, naso buco, mascara).
 - Manos (guantes).
 - Piel (ropa especial, uniforme, bata, gabacha, delantal).
 - Pies (calzado especial, botas cubre calzado).
4. Debe capacitar al personal y fortalecer las competencias sobre bioseguridad y gestión de riesgos biológicos.
5. Debe promover campañas sobre el bienestar emocional de los empleados.

F. Seguridad Industrial

Entre sus objetivos están: evitar lesiones y muerte por accidente, la reducción de los costos operativos de producción, contar con un sistema estadístico que permita detectar el avance o disminución de los accidentes y la causa de los mismos, así como contar con los medios necesarios para montar un plan de seguridad.

1. Debe tener definidas políticas de seguridad industrial en sus instalaciones.
2. Debe contar con un procedimiento que incluya las acciones a tomar ante cualquier circunstancia que represente riesgo industrial o riesgo de la carga (materiales no identificados).
3. Debe contar con planos actualizados de la empresa, en donde se detalle en forma impresa los siguientes puntos:
 - Los accesos de ingreso y salida de las instalaciones;
 - El área total donde se encuentren ubicadas sus instalaciones;

- Descripción del tipo de carga en cada área dentro de sus instalaciones, incluyendo la designación donde se encuentre la mercancía peligrosa, inflamable, de alto valor económico, entre otros;
 - Rutas de evacuación en caso de emergencia, incluyendo el procedimiento que señale los pasos a seguir para evacuar las instalaciones;
 - Ubicación física de los dispositivos electrónicos de seguridad que se utilicen en todas sus instalaciones, así como de las videocámaras, en su caso.
4. Ante el caso de pérdida del suministro eléctrico, debe disponer de un generador que proporcione energía al sistema de iluminación.
 5. Debe definir programas de mantenimiento del generador eléctrico que incluya un plan de contingencia ante un eventual desperfecto de este.
 6. Deber realizar inspecciones sin previo aviso sobre la observancia de los empleados a las normas de seguridad y deja registro de los hallazgos.
 7. Debe contar con una planificación para realizar simulacros de evacuación y/o actuación en situaciones de emergencia.
 8. Debe tener un plan de mantenimiento preventivo y correctivo de los dispositivos de seguridad de la empresa indicando la periodicidad de prueba de estos.

G. Seguridad Informática

Características y condiciones del sistema de procesamiento de datos y su almacenamiento, que garanticen su confidencialidad, integridad, disponibilidad y buen uso de la información que reside en el sistema de información.

1. Debe existir una estructura organizacional responsable de velar por la seguridad de información.
2. Debe tener establecidas políticas de confidencialidad y seguridad de la información con el personal.
3. Debe revisar los procedimientos de seguridad informática.
4. En caso de subcontratar o externalizar servicios informáticos, debe definir la política de seguridad y propiedad de la información.
5. El área informática debe contar con dispositivos de seguridad para resguardar el equipo.
6. Deben existir controles adecuados para el mantenimiento o servicio del equipo informático.
7. Debe contar con protección contra amenazas externas como ser: virus, hackers, entre otros.
8. Debe tener políticas establecidas de respaldos de información.
9. Debe tener controles de seguridad para accesos a red, como ser: firewalls, manejo de direcciones y servidores de autenticación

10. Debe tener políticas para el manejo de dispositivos removibles, tales como: CD/DVD, USB, Discos externos, tapes, diskettes, entre otros.
11. Debe llevar bitácoras transaccionales o históricas que permitan una adecuada trazabilidad.
12. Debe tener documentado un plan de contingencia para las tecnologías de información.
13. Debe tener políticas para la administración de usuarios y sus accesos.
14. Debe tener políticas en el sistema informático para el manejo de claves definidas periódicamente.
15. En caso de contar con acceso desde conexiones externas, debe definida una política.
16. Debería tener definida una política para el manejo de la propiedad intelectual.
17. Debe contar con servidor de datos electrónicos que contenga información referente al transporte o manejo de la carga, se resguarda en un ambiente seguro.

H. Seguridad de la carga

Los aspectos más críticos, en cuanto a seguridad y fiabilidad para la correcta manipulación y transporte de las mercancías, se refieren, entre otros, a las condiciones especiales de transporte que requieren ciertos productos, a los robos o hurtos de mercancías en la cadena, y a la correcta estiba y manipulación de las mercancías. También a la instalación de dispositivos de control de acceso para impedir el daño o desaparición de mercancías.

1. Debe contar con un procedimiento documentado sobre la seguridad de las mercancías.
2. Debe llevar inventario de las mercancías que tenga como mínimo la información siguiente: peso, fecha de ingreso, cantidad y descripción (las mercancías almacenadas deben ser identificadas por medio de marcas o etiquetas u otro medio de control).
3. Debe llevar un control electrónico o procedimiento que permita establecer la ubicación física de la carga de importación, de exportación o en tránsito dentro de las instalaciones, así como la mercancía que es objeto de carga o descarga.
4. El material que se utiliza para el envasado, empaque o embalaje de las mercancías debe ser controlado y revisado antes de ser utilizado.
5. Los contratos con los socios comerciales que tengan relación con las mercancías deben contar con cláusulas de responsabilidad y controles para garantizar la seguridad de la carga.
6. Debe contar con un encargado que lleve un registro del tipo de mercancía y de las personas involucradas en la operación de carga, descarga, y la información se debe almacenar en un archivo de reportes.
7. Debe contar con un circuito cerrado de televisión que monitoree el proceso de carga, descarga y almacenaje de las mercancías.
8. Debe tener un registro fotográfico del proceso de la carga y/o descarga de las mercancías, que incluya fotografías del contenedor y sellos de seguridad.

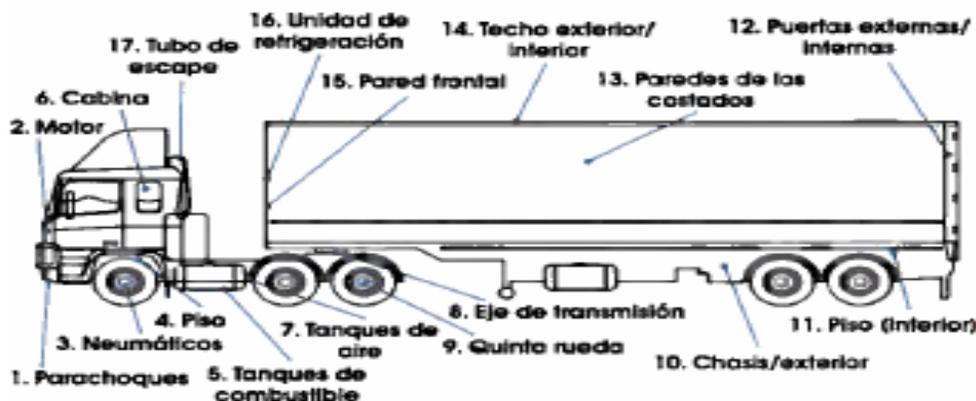
9. Las puertas de ingreso y salida del área de carga, descarga y almacenamiento de la mercancía deben contar con dispositivos de cierre.
10. Debe tener un procedimiento documentado para la identificación de los conductores antes de que reciban o entreguen la carga.
11. Debe tener un procedimiento documentado para investigar y solucionar los casos de sobrantes o faltantes y otras discrepancias o anomalías relacionadas con la carga.
12. Debe contar con controles conforme a las regulaciones nacionales sobre las sustancias precursoras para la fabricación de los productos utilizados en los diferentes procesos.

I. Transporte de la Carga

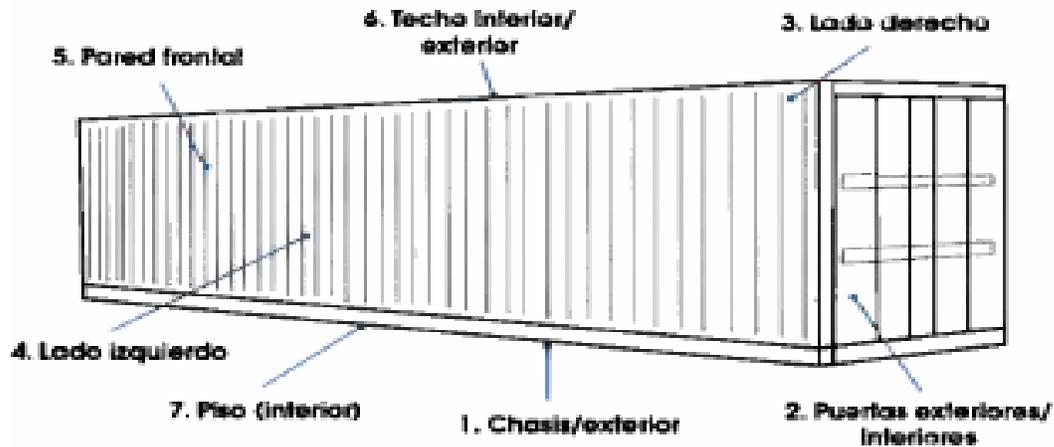
Se debe mantener la integridad del contenedor y del remolque para la protección contra la introducción de materiales o de personas no autorizadas. Los procedimientos deben aplicarse en el lugar donde se llenen, para sellarlos adecuadamente y mantener la integridad de los contenedores para transporte y remolque.

1. Debe tener un procedimiento documentado para la seguridad del medio de transporte.
2. Sus socios comerciales deben utilizar procedimientos que le permitan garantizar la seguridad de los medios de transporte en el manejo de la carga.
3. Si el transportista contratado, subcontrata los servicios de un tercero, debe asegurarse que estos cumplan con los mismos criterios de seguridad.
4. Debe contar con un procedimiento para sellar correctamente y para mantener la integridad del envío en los medios de transporte
5. Los contenedores, furgones, camiones y cualquier otro vehículo destinado el transporte de mercancías, deben ser revisados conforme a un procedimiento de inspección como:

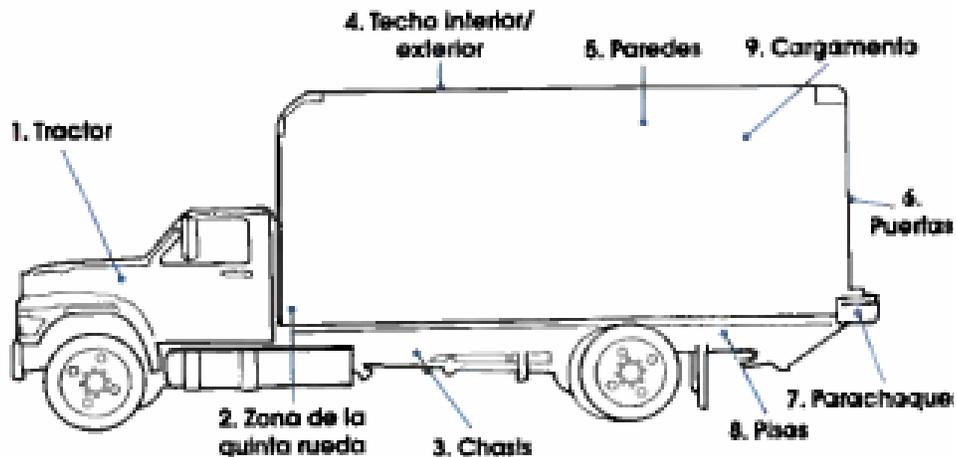
Puntos de inspección del tractor y del remolque



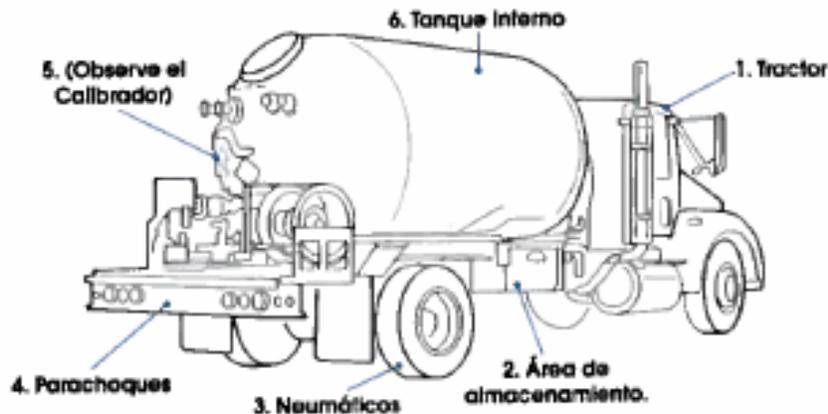
Puntos de inspección del contenedor



Puntos de inspección de camiones con cajas, vagoneta tipo van o vagoneta de Carga



Puntos de inspección de la Cisterna de Propano



6. Debe tener un sistema que permita registrar electrónicamente o documentalmente las actividades de transporte, tales como: contratos emitidos de transportes, asignación de medios de transportes, registro de mercancías a transportarse y mercancías entregadas.
7. Debe tener controles que permitan documentar la trazabilidad de las mercancías e informar a la autoridad aduanera en caso de existir alguna irregularidad.
8. Los contenedores, furgones, camiones o cualquier otro medio de transporte que se encuentren vacíos o cargados deben permanecer debidamente controlados y ubicados en un lugar alejado de las áreas de carga y descarga.
9. Cualquier reparación o mantenimiento realizados a las unidades de transporte, contenedores, furgones, camiones, etc., deben ser registradas en una bitácora que indique el nombre del técnico, fecha, hora y descripción de la reparación.
10. Debe tener procedimientos documentados a aplicar por el conductor del medio de transporte sobre políticas de seguridad en la carga, descarga y durante el transporte de esta; lugares de parqueo o de descanso, abastecimiento, tiempos y/o restricciones durante el transporte.
11. Debe tener un programa de mantenimiento correctivo y preventivo para los medios de transporte.
12. Debe tener un procedimiento documentado para neutralizar y denunciar la entrada no autorizada a los contenedores o furgones en el área de almacenaje de estos.
13. Debe tener un sistema de control del medio de transporte que permita monitorear la unidad en cualquier momento, de preferencia dispositivos de control GPS.
14. La empresa debe contar con una copia impresa o electrónica de los documentos de transporte completos y legibles.
15. Debe convenir con sus socios comerciales la inspección de contenedores vacíos, de furgones y camiones para mantener su integridad y la seguridad de la carga.

16. Debe implementar medidas de seguridad que restrinjan el acceso a los documentos de transporte.

J. Marchamos o Precintos

Procedimientos escritos sobre la posesión, manejo y uso de sellos, así como para reconocer y reportar sellos y/o contenedores comprometidos a la autoridad correspondiente.

1. Debe tener un procedimiento documentado para el registro, control, almacenamiento, inventario y disposición final de los sellos de seguridad, precintos o marchamos para los medios de transporte.
2. Debe contar con un procedimiento documentado que incluya las acciones a seguir en el caso de sellos de seguridad, marchamos o precintos con indicios de manipulación ilícita.
3. Debe tener un procedimiento documentado que incluya, entre otras, las normas de tratamiento para el desecho de los sellos de seguridad, marchamos o precintos utilizados o inutilizados.
4. Los marchamos o precintos que se utilicen para asegurar la carga deben cumplir con las normas ISO vigente (Norma ISO/PAS 17712).
5. Los sellos de seguridad, precintos o marchamos que se utilizan en los vehículos de transporte de carga deben estar resguardados en un ambiente cerrado y con acceso sólo por el personal autorizado.
6. Debe definir un responsable para autorizar y asignar a las personas que tendrán acceso a estos dispositivos y lleva un control del inventario.

NOTA. Es indispensable para todos los procedimientos:

1. Estar documentado en papel o electrónicamente.
2. Tener establecido un responsable y un sustituto para su aplicación.
3. Estar implementados, que sean verificables y que se pueda comprobar su aplicación.
4. Ser utilizados en las diferentes instalaciones, si existieren.
5. Aplicarse sin que se entorpezca el funcionamiento normal de la empresa.
6. Observarse mejoría con su aplicación.
7. Tener previsto modelos de comunicaciones con la Aduana y con los demás Operadores sobre cualquier incidencia importante o consulta a realizar.
8. Llevar un registro de modificaciones, con la fecha, versión y lo modificado.
9. Ser conocidos por todo el personal que labora en la empresa (los que sean de aplicación general), y los que se aplican en áreas específicas, al personal que le compete.
10. Estar en constante revisión, para:
 - a. Mejorarlos

- b. Actualizarlos
- c. Modificarlos, por irregularidades e incidencias que se produzcan, para evitar vuelvan a repetirse.

V. GLOSARIO DE TERMINOS

- **Amenaza:** Son aquellos factores externos a la organización que advierten proximidad o propensión a un evento de pérdida (materialización de riesgo) sobre los cuales esta no tiene control.
- **Análisis y evaluación de riesgo:** Uso sistemático de la información disponible para determinar las posibles amenazas, sus causas, probabilidad de manifestación y la magnitud de sus consecuencias.
- **Asociados de negocios:** Cliente, proveedor o tercero vinculado a la cadena logística considerado con algún nivel de criticidad de acuerdo con el modelo de gestión de riesgo de la organización.
- **Bioseguridad:** Conjunto de medidas de protección, promoción y prevención, destinadas a mantener la salud y seguridad frente a los factores y agentes biológicos.
- **Cadena logística:** Está integrada por todos los medios y métodos necesarios para llevar a cabo la organización de una empresa, o de un servicio
- **Control:** Actividad de seguimiento del desarrollo y etapas de los procesos en la cadena logística, para asegurar el resultado esperado y tomar medidas preventivas, correctivas y de mejora, para reducir la materialización de un riesgo.
- **Cliente:** Organización o persona que recibe un producto o servicio (consumidor, usuario final, minorista, beneficiario y comprador. El cliente puede ser interno o externo a la organización).
- **Corrección:** Acción tomada para corregir una no conformidad detectada.
- **Debe:** Requisito de carácter obligatorio para demostrar la conformidad del sistema de gestión en control en seguridad.
- **Debería:** Requisito de carácter condicional de la cual la organización deberá justificar la exclusión para demostrar la conformidad del sistema de gestión en control en seguridad.
- **Documento:** Información y su medio de soporte o registro, especificación, procedimiento documentado, plano, informe, norma. El medio de soporte puede ser papel, disco magnético, óptico o electrónico, fotografía o muestra patrón o una combinación de estos.
- **Disposición:** Precepto legal o reglamentario, orden o mandato.
- **Establecer:** Hacer que empiece a funcionar una cosa o una actividad, generalmente con propósito de continuidad (crear, fundar).
- **Estructura de la organización:** Disposición de responsabilidades, autoridades y relaciones entre el personal.

- **Factores externos:** Son las fuerzas que se generan fuera de la organización, que inciden en los asuntos de control y seguridad y que deben tenerse en cuenta de manera apropiada; incluye aspectos como: legislación, innovaciones tecnológicas y normatividades sectoriales.
- **Factores internos:** Son los aspectos de la organización que inciden en su capacidad para cumplir con la gestión de control y seguridad; incluye aspectos como: reorganización interna, cambio en la tecnología, cultura en materia de prevención de riesgos y modificaciones a procesos.
- **Gestión de riesgo:** Proceso definido para identificar, analizar, tratar, monitorear y controlar la exposición y las consecuencias de los diferentes riesgos que puedan afectar negativamente a las personas, activos, y procesos de la organización.
- **Gestión en seguridad:** Conjunto de actividades encaminadas a la prevención y protección de los riesgos a que están expuestas personas, activos y procesos, de las organizaciones.
- **Hallazgo:** Resultados de la evaluación de la evidencia objetiva, recopilada frente al cumplimiento de la lista de obligaciones. Los hallazgos pueden indicar tanto el cumplimiento como el no cumplimiento de los requisitos o generar observaciones para posterior seguimiento futuro.
- **Incidencia:** Influencia o efecto que tiene una cosa sobre otra.
- **Infraestructura:** Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización.
- **Inspección:** Evaluación de la conformidad por medio de observación y dictamen, acompañada cuando sea apropiado por medición, ensayo/prueba o comparación con patrones.
- **Organización:** Persona natural o jurídica, pública o privada, que tiene sus propias funciones, responsabilidades y administración en la cadena logística y que se habilita o se habilitará como OEA.
- **Planes de contingencia;** Son los procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir el normal funcionamiento de esta, aun cuando alguna de sus funciones se viese dañada por un accidente o incidente, interno o externo.
- **Planes de emergencia:** Es la respuesta integral que involucra a toda la empresa, con el compromiso de directivos y empleados en permanente acción para responder oportuna y eficazmente con las actividades correspondientes al antes, durante y después de una emergencia.
- **Política de seguridad:** Intenciones globales de una organización relativas a un compromiso de seguridad y prevención de riesgos, cuya aplicación está orientada y hace referencia para el establecimiento del Programa OEA.
- **Procedimiento:** Método estándar lógico y ordenado en que se ejecutan las actividades para obtener siempre el mismo resultado, y generando evidencia objetiva de cumplimiento de los controles de seguridad aplicados (puede estar documentado o no).

- **Procedimiento documentado:** Cuando el término aparece significa que un método estándar, lógico y ordenado sea establecido, documentado, implementado y mantenido en la organización.
- **Proceso:** Conjunto de actividades que se realizan o suceden ordenadamente bajo ciertas circunstancias, mediante las cuales los elementos de entrada se transforman en resultados.
- **Propiedad intelectual:** Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano.
- **Registro:** Documenta que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.
- **Requisito:** Necesidad o expectativa establecida por la norma, el estándar, la organización o la legislación aplicable al OEA, generalmente implícita u obligatoria.
- **Simulacro:** Es la simulación de una situación de emergencia donde se busca recrear, de una manera ficticia, las dificultades que se generarían en una situación real.
- **Trazabilidad:** Capacidad para seguir la historia, la aplicación o la localización de todo aquello que está bajo consideración.
- **Validación:** Acción por la cual se confirma mediante el suministro de evidencia objetiva que se han cumplido, se aplican y se mantienen los criterios mínimos de seguridad establecidos para los OEA.
- **Vulnerabilidad:** Son todos los factores internos a la organización que facilitan la materialización de un evento de pérdida (riesgos) sobre los cuales se deberán determinar alternativas de control.