NORMA CUBANA

NC

ISO 28001: 2015
(Publicada por la ISO en 2007)

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO — BUENAS PRÁCTICAS PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO, EVALUACIONES Y PLANES — REQUISITOS Y GUÍA
(ISO 28001: 2007, IDT)

Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

ICS: 47.020.99

1. Edición Octubre 2015

Oficina Nacional de Normalización (NC) Calle E No. 261 El Vedado, La Habana. Cuba. Teléfono: 78300835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC), es el Órgano Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 51 de Seguridad y protección de las instalaciones, integrado por representantes de las siguientes entidades.

  - Ministerio del Interior (MININT)
  - Oficina del Historiador de La Habana (OHLH)
  - Ministerio de Relaciones Exteriores (MINREX)
  - Ministerio de Energía y Minas (MINEM)
  - Instituto Nacional de Recursos Hidráulicos (INRH)
  - Ministerio del Turismo (MINTUR)
  - Ministerio de la Construcción (MICONS)
  - Ministerio de Salud Pública (MINSAP)
  - Ministerio de Comunicaciones (MICOM)
  - Ministerio del Transporte CACSA (MITRANS)
  - Banco Central de Cuba (BCC)
  - Aduana General de la República. (AGR)

- Es una adopción idéntica por el método de endoso de la versión en español de la Norma Internacional ISO 28001: 2007 *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance.*

- Incluye los Anexos A, B y C informativos.

ÍNDICE

Página

PRÓLOGO

ISO (la Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de las normas internacionales normalmente se realiza a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para su votación. La publicación como norma internacional requiere la aprobación por al menos el 75% de los organismos miembros con derecho a voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta norma internacional puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La Norma Internacional ISO 28001 fue preparada por el Comité Técnico ISO/TC 8, *Embarcaciones y tecnología marina*, en colaboración con otros comités técnicos relevantes responsables de nodos específicos de la cadena de suministro.

Esta primera edición de la Norma ISO 28001 anula y sustituye al ISO/PAS 28001:2006, que se ha revisado técnicamente.

INTRODUCCIÓN

Los incidentes de la seguridad contra las cadenas de suministro internacionales son amenazas al comercio internacional y al crecimiento económico de los países comerciantes. Las personas, los bienes, la infraestructura y el equipamiento – incluyendo los medios de transporte - deben protegerse contra los incidentes de seguridad y sus efectos potencialmente devastadores. Dicha protección beneficia a la economía y a la sociedad como un todo.

Las cadenas de suministro internacionales son altamente dinámicas y constan de muchas entidades y socios de negocio. Esta norma internacional reconoce esta complejidad. Se ha desarrollado para permitir que una organización individual en la cadena de suministro aplique sus requisitos en conformidad con el modelo de negocio particular de la organización y con su función en la cadena de suministro internacional.

Esta norma internacional proporciona una opción para que las organizaciones establezcan y documenten niveles razonables de seguridad dentro de la cadena de suministro internacional y sus componentes. Permitirá a dichas organizaciones tomar mejores decisiones basadas en el riesgo relativo a la seguridad de aquellas cadenas de suministro internacionales.

Esta norma internacional es multimodal y se quiere que esté de acuerdo con y complemente al Marco de normas de la Organización Mundial de Aduanas (OMA) para asegurar y facilitar el comercio global (Marco). No pretende cubrir, reemplazar o anular a los programas de seguridad de las cadenas de suministro de las agencias de aduanas individuales ni sus requisitos de certificación y validación.

El uso de esta norma internacional ayudará a una organización a establecer niveles adecuados de seguridad dentro de aquellas partes de una cadena de suministro internacional que controle. También servirá de base para determinar o validar el nivel de seguridad existente en dichas cadenas de suministro de la organización mediante auditores internos o externos o mediante aquellas agencias gubernamentales que elijan utilizar el cumplimiento con esta norma internacional como la base para la aceptación en sus programas de seguridad de la cadena de suministro. Los clientes, socios, agencias gubernamentales y otros podrían solicitar a las organizaciones que afirman el cumplimiento con esta norma internacional que realicen una auditoría o una validación que confirme dicho cumplimiento. Las agencias gubernamentales podrían acordar mutuamente aceptar las validaciones realizadas por otras agencias gubernamentales. Si se va a llevar a cabo una auditoría por una tercera parte, entonces la organización necesita considerar el emplear un tercer organismo de certificación acreditado por un organismo competente, que sea miembro del Foro Internacional de Acreditación (véase el anexo C).

No es intención de esta norma internacional duplicar los requisitos gubernamentales y las normas relativas a la seguridad de la cadena de suministro en cumplimiento con el Marco OMA SAFE. Las organizaciones que ya se hayan certificado o validado mediante el reconocimiento mutuo de los gobiernos son cumplidoras de esta norma internacional.

Los datos de salida resultantes de esta norma internacional serán los siguientes.

- Una Declaración de Cobertura que defina los límites de la cadena de suministro cubierta por el plan de seguridad.
- Una Evaluación de la Seguridad que documente las vulnerabilidades de la cadena de suministro para definir los escenarios de amenazas a la seguridad. También describe los impactos que se pueden esperar razonablemente de cada potencial escenario de amenazas a la seguridad.
- Un Plan de Seguridad que describa las medidas de seguridad establecidas para gestionar los escenarios de amenazas a la seguridad identificados por la evaluación de la Seguridad.
- Un programa de formación que establezca cómo se entrenará al personal de seguridad para cumplir con sus tareas asignadas relativas a la seguridad.

Para llevar a cabo la evaluación de la seguridad, necesaria para generar un plan de seguridad, una organización que use esta norma internacional:

– identificará las amenazas planteadas (escenarios de amenazas a la seguridad);

– determinará con qué probabilidad las personas podrían transformar cada escenario de amenazas a la seguridad identificado por la Evaluación de la Seguridad en un incidente de seguridad.

Esta determinación se hace mediante la revisión del estado vigente de la seguridad en la cadena de suministro. Basado en los hallazgos de esa revisión, se usa el juicio profesional para identificar lo vulnerable que es la cadena de suministro para cada escenario de amenazas a la seguridad.

Si se considera la cadena de suministro inaceptablemente vulnerable para un escenario de amenazas a la seguridad, la organización desarrollará procedimientos adicionales o cambios operacionales para disminuir la probabilidad, la consecuencia o ambas. Estos procedimientos o cambios se llaman contramedidas. Basadas en un sistema de prioridades, las contramedidas necesitan incorporarse al plan de seguridad para reducir la amenaza a un nivel aceptable.

Los anexos A y B son ejemplos ilustrativos de los procesos de seguridad basados en la gestión de riesgos para proteger a personas, activos y misiones de la cadena de suministro internacional. Facilitan un macro-enfoque para las cadenas de suministro complejas y/o enfoques más discretos de partes de ellas.

También se quiere que estos anexos

– faciliten el entendimiento, adopción e implementación de metodologías, que pueden ser adaptadas por las organizaciones;

– proporcionen orientación para una gestión de la seguridad base para la mejora continua;

– asista a las organizaciones a gestionar los recursos para tratar los riesgos de la seguridad existentes y emergentes;

– describa los posibles medios de evaluación del riesgo y la mitigación de las amenazas a la seguridad en la cadena de suministro desde la situación de las materias primas hasta el almacenaje, fabricación y transporte de los bienes terminados hasta el mercado.

El anexo C proporciona una guía para obtener el consejo y la certificación para esta norma internacional si una organización que la utilice elige ejercer esta opción.

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma internacional proporciona requisitos y sirve de guía a las organizaciones en las cadenas de suministro internacionales para:

– desarrollar e implementar procesos de seguridad en la cadena de suministro;

– establecer y documentar un nivel mínimo de seguridad en la cadena o cadenas de suministro o en una parte de una cadena de suministro;

– asistir en el cumplimiento del criterio del Operador Económico Autorizado (OEA) aplicable, establecido en el Marco de la Organización de Aduanas y en la conformidad con los programas nacionales de seguridad en la cadena de suministro.

NOTA Sólo un miembro de la Agencia Nacional de Aduanas puede designar a organizaciones como OEA de acuerdo con sus programas de seguridad de la cadena de suministro y con los requisitos esperados de certificación y validación.

Además, esta norma internacional establece ciertos requisitos de documentación que permitirían su verificación.

Los usuarios de esta norma internacional

– definirán la parte de una cadena de suministro internacional en la que hayan establecido la seguridad (véase el apartado 4.1);

- llevarán a cabo evaluaciones de la seguridad en esa parte de la cadena de suministro y desarrollarán las contramedidas adecuadas;
- desarrollarán e implementarán un plan de seguridad para la cadena de suministro;
- formarán al personal de seguridad en sus tareas relacionadas con la seguridad.

2 NORMAS PARA CONSULTA

Las normas que a continuación se indican son indispensables para la aplicación de esta norma. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

ISO 20858 *Embarcaciones y tecnología marinas. Evaluaciones de la seguridad de las instalaciones portuarias marítimas y desarrollo del plan de seguridad.*

Convención Internacional para la Seguridad de la Vida en el Mar (CISVM) [*International Convention for the Safety of Life at Sea (SOLAS)*], 1974, Organización Marítima Internacional.

3 TÉRMINOS Y DEFINICIONES

Para los fines de este documento, se aplican los siguientes términos y definiciones.

3.1 autoridad y otros funcionarios gubernamentales apropiados:
Aquel personal gubernamental y de la autoridad que tiene jurisdicción legal específica sobre la cadena de suministro internacional o sobre partes de la misma.

3.2 activo(s):
Planta, maquinaria, propiedad, edificios, vehículos, barcos, aviones, medios de transporte y otros elementos de la infraestructura o la planta y sistemas relacionados que tienen una función o servicio de negocio clara y cuantificable.

NOTA Esta definición incluye cualquier sistema de información que es integral para la cesión de la seguridad y la aplicación del sistema de gestión.

3.3 operador económico autorizado:
Parte implicada en el movimiento internacional de bienes en cualquier función que haya sido aprobada por una administración de aduanas nacional o en su nombre como cumplidora con la OMA o con normas equivalentes de la seguridad de la cadena de suministro.

NOTA 1 Operador económico autorizado es un término definido en el Marco de normas de la Organización Mundial de Aduanas.

NOTA 2 Los operadores económicos autorizados incluyen a los fabricantes *inter alia*, los importadores, los exportadores, los agentes, los transportistas, los consolidadores, los intermediarios, los puertos, los aeropuertos, los operadores terminales, los operadores integrados, los almacenes y los distribuidores.

3.4 socio:
Aquellos contratistas, suministradores o proveedores de servicio que una organización contrata para ayudar a la organización en su función como una **organización en la cadena de suministro** (3.15).

3.5 unidad de transporte de carga:
Vehículo de transporte por carretera, vagón de transporte ferroviario, contenedor de transporte, vehículo cisterna por carretera, vagón cisterna ferroviario o cisterna transportable.

3.6 consecuencia:
Pérdida de vida, daño a la propiedad o trastorno económico, incluyendo el trastorno a los sistemas de transporte, que puede esperarse razonablemente como el resultado de un ataque a una organización en la cadena de suministro o por medio del uso de la cadena de suministro como un arma.

3.7 transporte:
Instrumento físico del comercio internacional que traslada bienes de un lugar a otro.

EJEMPLOS Caja, palé, unidad de trasporte de carga, equipo de manipulación de carga, camión, barco, avión y tren.

3.8 contramedidas:
Acciones que se toman para disminuir la probabilidad de que un escenario de amenazas a la seguridad consiga sus objetivos, o para reducir las consecuencias probables de un escenario de amenazas a la seguridad.

3.9 custodia:
Periodo de tiempo en el que una organización en la cadena de suministro controla directamente la fabricación, el procesado, la manipulación y el transporte de bienes y la información relativa a su envío dentro la cadena de suministro.

3.10 aguas abajo:
Manipulación, procesos y movimientos de bienes cuando ya no están bajo la custodia de la organización en la cadena de suministro.

3.11 bienes:
Aquellos elementos o materiales que, al establecimiento de una orden de compra, se fabrican, procesan, manipulan o transportan en la cadena de suministro para el uso o consumo por parte del comprador.

3.12 cadena de suministro internacional:
Cadena de suministro que en algún punto cruza una frontera internacional o económica.

NOTA 1 Todas las partes de esta cadena se consideran internacionales desde el momento en que se cierra una orden de compra hasta que esos bienes pasan el control de aduanas del país o la economía de destino.

NOTA 2 Si el paso de aduanas se ha eliminado mediante acuerdos o tratados regionales de países o economías específicos, el final de la cadena de suministro es el puerto o la entrada al país o a la economía en la que los bienes habrían pasado la aduana si los acuerdos o tratados no hubieran estado establecidos.

3.13 probabilidad:
Facilidad o dificultad con la que un escenario de amenazas a la seguridad podría progresar hasta convertirse en un incidente de seguridad.

NOTA La probabilidad se evalúa basándose en la resistencia que oponen los procesos de seguridad establecidos frente a un incidente de seguridad que implique al escenario de amenazas a la seguridad que se examina y se expresa cualitativa o cuantitativamente.

3.14 sistema de gestión:
Estructura de la organización para gestionar sus procesos o actividades que transforma entradas de recursos en un producto o servicio, que cumple los objetivos de la organización.

NOTA No se pretende que esta norma internacional especifique un sistema de gestión específico o que requiera la creación de un sistema de gestión de la seguridad separado. La Norma ISO 9001 (Sistemas de Gestión de la Calidad), la Norma ISO 14001 (Sistemas de Gestión Ambiental), la Norma ISO 28000 (Sistemas de gestión de la seguridad para la cadena de suministro) y el Código Internacional de Gestión de la Seguridad (ISM) son algunos ejemplos de sistemas de gestión.

3.15 organización en la cadena de suministro:
Cualquier entidad que:

- fabrica, manipula, procesa, carga, consolida, descarga o recibe bienes al establecimiento de una orden de compra que en algún punto cruza una frontera internacional o económica;
- transporta bienes por cualquier medio en la cadena de suministro internacional independientemente de si su segmento particular de la cadena de suministro cruza fronteras nacionales (o económicas); o
- proporciona, gestiona o conduce la generación, distribución o el flujo de información relativa al envío usado por las agencias de aduanas o en las prácticas de negocios.

3.16 gestión del riesgo:
Proceso de toma de decisiones de gestión basadas en un análisis de las posibles amenazas, sus consecuencias, y la probabilidad de que sucedan.

NOTA Un proceso de gestión del riesgo se inicia normalmente con el propósito de optimizar la distribución de recursos de la organización necesaria para operar en un entorno particular.

3.17 campo de aplicación del servicio:
Función o funciones que desarrolla una organización en la cadena de suministro, y el lugar en el que desarrolla esta o estas funciones.

3.18 declaración de seguridad:
Documento acordado con un socio, que especifica las medidas de seguridad implementadas por ese socio, incluyendo, como mínimo, cómo se salvaguardan los bienes e instrumentos físicos del comercio internacional, cómo se protegen la información asociada y cómo se demuestran y verifican las medidas de seguridad.

NOTA La organización la utilizará en la cadena de suministro para evaluar la adecuación de las medidas de seguridad relativas a la seguridad de los bienes.

3.19 plan de seguridad:
Disposiciones planificadas para asegurarse de que la seguridad se gestiona adecuadamente.

NOTA 1 Se diseña para asegurar la aplicación de medidas que protejan la organización de un incidente de seguridad.

NOTA 2 Se puede añadir el plan a otros planes operacionales.

3.20 seguridad:
Resistencia a actos intencionados destinados a causar daño o perjuicio a la cadena de suministro o a través de ella.

3.21 incidente de seguridad:
Cualquier acto o circunstancia que produce una **consecuencia** (3.6).

3.22 personal de seguridad:
Aquellas personas de la organización en la cadena de suministro a las que se han asignado tareas relativas a la seguridad.

NOTA Estas personas pueden ser o no empleados de la organización.

3.23 información reservada de la seguridad; materiales reservados de la seguridad:
Información o materiales, producidos por los procesos de seguridad de la cadena de suministro o incorporados a ella, que contienen información sobre los procesos de seguridad, envíos o directrices gubernamentales que podrían no estar disponibles para el público y que sería útil para alguien que quisiera iniciar un incidente de seguridad.

3.24 cadena de suministro:
Conjunto relacionado de recursos y procesos que al establecimiento de una orden de compra se inicia con el aprovisionamiento de materia prima y se extiende a lo largo de la fabricación, procesado, manipulación y entrega de bienes y servicios relacionados al comprador.

NOTA La cadena de suministro puede incluir a los vendedores, las instalaciones de fabricación, los proveedores logísticos, los centros de distribución interna, los distribuidores, los mayoristas y otras entidades implicadas en la fabricación, el procesado, la manipulación y la entrega de los bienes y de sus servicios relacionados.

3.25 meta:
Personal, medios de transportes, bienes, activos físicos, procesos de fabricación y sistemas de manipulación, control o documentación en una organización en la cadena de suministro.

3.26 escenario de amenazas a la seguridad:
Medios por los que un potencial incidente de seguridad podría ocurrir.

3.27 aguas arriba:
Manipulación, procesos y movimientos de bienes que ocurren antes de que la organización en la cadena de suministro tenga la custodia de los bienes.

3.28 Organización Mundial de Aduanas; OMA:
Organismo intergubernamental independiente cuya misión es aumentar la eficacia y la eficiencia de las administraciones de aduanas.

NOTA Es la única organización mundial intergubernamental competente en asuntos de aduanas.

4 ÁMBITO DE APLICACIÓN

4.1 Declaración de aplicación

La organización en la cadena de suministro debe describir la parte de la cadena de suministro internacional que alega estar en cumplimiento con esta norma internacional en una Declaración de Aplicación. La Declaración de Aplicación debe incluir al menos la siguiente información:

a) detalles de la organización;

b) alcance del servicio;

c) nombres e información de contacto de todos los socios en el alcance del servicio definido;

d) fecha en la que se completó la evaluación de la seguridad y periodo de validez de la evaluación de la seguridad; y

e) firma de una persona autorizada para firmar en nombre de esa organización.

Las organizaciones en la cadena de suministro pueden ampliar la Declaración de Aplicación para incluir otras partes de la cadena de suministro, por ejemplo incluyendo el destino final.

4.2 Socios

Si en la cadena de suministro descrita en la Declaración de Aplicación la organización utiliza socios, la organización debe, sujeta al apartado 4.3 y al apartado 4.4, requerir a dichos socios que proporcionen una declaración de seguridad. La organización debe considerar esta declaración de seguridad en su evaluación de la seguridad y puede requerir que se ejecuten contramedidas específicas.

4.3 Certificados o aprobaciones aceptados internacionalmente

Las compañías de transportes y las instalaciones, que tengan certificados o aprobaciones aceptados internacionalmente, expedidos con arreglo a convenciones internacionales obligatorias que rigen la seguridad de los distintos sectores del transporte, tendrán implementadas prácticas, planes y procesos de seguridad que cumplan los requisitos aplicables de esta norma internacional y que no necesitan ser auditados para confirmar dicho cumplimiento. Para las compañías navales, los barcos y las instalaciones portuarias, cuando sea aplicable, los certificados o aprobaciones se deben expedir de acuerdo con SOLAS XI-2/4 o SOLAS XI-2/10.

De conformidad con el capítulo 1, las agencias nacionales de aduanas pueden, además de la posesión de certificados de seguridad o aprobaciones internacionalmente aceptados, requerir que se implementen medidas y prácticas de seguridad adicionales por parte de las compañías de transportes y las instalaciones como una condición para su designación como un OEA.

4.4 Exención de los socios del requisito de declaración de seguridad

Aquellos socios que confirman a la organización que:

a) se ha verificado que cumplen con esta norma internacional o con la Norma ISO 20858,

b) están cubiertos por el apartado 4.3, o

c) se les ha designado como OEA de acuerdo con el programa de seguridad de la cadena de suministro de una agencia nacional de aduanas, el cual se ha determinado que está de acuerdo con el Marco OMA SAFE,

deben aparecer en la Declaración de Aplicación. Sin embargo, la organización no necesita realizar evaluaciones de la seguridad adicionales para dichos socios o requerir que aporten declaraciones de seguridad.

4.5 Revisiones de la seguridad de los socios

A excepción de los socios cubiertos por el apartado 4.3 o el apartado 4.4, la organización en la cadena de suministro debe realizar revisiones de los procesos e instalaciones de sus socios para determinar la validez de sus declaraciones de seguridad. El alcance y la frecuencia de estas revisiones se deben determinar a través de un análisis de los riesgos implicados. La organización debe mantener los resultados de estas revisiones.

NOTA Para facilitar la lectura, la organización que solicita el cumplimiento, incluyendo aquellas partes de su cadena de suministro operadas por socios que cumplen o no esta norma internacional, se denomina en los siguientes párrafos como "la organización", a no ser que por la claridad se precise otra cosa.

5 PROCESOS DE SEGURIDAD DE LA CADENA DE SUMINISTRO

5.1 Generalidades

Se requiere a las organizaciones en cadenas de suministro internacionales que han adoptado esta norma internacional tanto que gestionen la seguridad a lo largo de su parte de la cadena de suministro como que tengan un sistema de gestión establecido para mantener ese objetivo. Esta norma internacional requiere que se establezcan e implementen prácticas y/o procesos de seguridad para reducir el riesgo de actividades que podrían conducir a incidentes de seguridad de la cadena de suministro internacional.

Las organizaciones en la cadena de suministro que buscan el cumplimiento con esta norma de seguridad deben tener un plan de seguridad basado en el resultado de la evaluación de la seguridad que documente la existencia de medidas y procedimientos de seguridad e incorpore contramedidas, cuando sean aplicables, para la parte de la cadena de suministro internacional que han incluido en su Declaración de Aplicación.

5.2 Identificación del alcance de la evaluación de la seguridad

El alcance de la evaluación de la seguridad debe incluir todas las actividades desarrolladas por la organización tal como se describa en su Declaración de Aplicación (véase el apartado 4.1). Se debe llevar a cabo la evaluación periódicamente y se debe revisar el plan de seguridad cuando sea apropiado. Se deben documentar y conservar los resultados de la evaluación.

La evaluación de la seguridad también debe cubrir los sistemas de información, los documentos y las redes concernientes a la manipulación y movimiento de bienes mientras estén bajo la custodia de la organización. Los acuerdos de seguridad existentes deben, sujetos al apartado 4.3 y al apartado 4.4, evaluarse en todos los puntos y para todos los socios cuando haya potenciales vulneraciones de la seguridad.

5.3 Realización de la evaluación de la seguridad

5.3.1 Personal de evaluación

La persona o equipo que realiza la evaluación de la seguridad debe tener colectivamente habilidades y conocimientos que incluyan, pero no se limiten, a lo siguiente:

- técnicas de evaluación de riesgos aplicables a todos los aspectos de la cadena de suministro internacional, desde el punto en que la organización en la cadena de suministro toma la custodia de los bienes hasta el punto en que los bienes ya no están bajo la custodia de la organización o abandonan la cadena de suministro internacional;
- la aplicación de las medidas apropiadas para evitar la revelación no autorizada de material reservado de seguridad, o el acceso al mismo;
- cuando sea apropiado, las operaciones y procedimientos implicados en la fabricación, la manipulación, el procesado, el movimiento y/o la documentación de los bienes;
- las medidas de seguridad relacionadas con el envío, el transporte, el personal, los locales, y con los sistemas de información en esa parte aplicable de la cadena de suministro;
- una comprensión de las amenazas a la seguridad y de las metodologías de mitigación;
- la comprensión de esta norma internacional.

Se debe documentar el nombre de la persona o los nombres de los miembros del equipo que realiza la evaluación así como de sus capacitaciones.

5.3.2 Proceso de evaluación

La organización debe establecer, implementar y mantener uno o varios procedimientos para identificar las contramedidas existentes para mitigar las amenazas a la seguridad. La organización debe elaborar una relación de escenarios de amenazas a la seguridad, incluyendo aquéllos considerados necesarios por los funcionarios gubernamentales apropiados. Si los funcionarios gubernamentales no han tomado parte, esto se debe documentar en la evaluación de la seguridad.

Para cada escenario de amenazas a la seguridad, la organización debe evaluar las contramedidas existentes y determinar la probabilidad y las consecuencias relevantes para cada escenario de amenazas a la seguridad y evaluar la necesidad de contramedidas adicionales para reducir el riesgo de la seguridad a un nivel aceptable.

La organización debe revisar la declaración o declaraciones de seguridad proporcionadas por cada socio, como se define en el apartado 4.2, y aplicar el juicio profesional, el conocimiento de la entidad o entidades y/o los requisitos de las agencias reglamentarias. Para determinar la aceptación de la declaración de seguridad, también se puede obtener y utilizar cualquier otra información disponible.

Las organizaciones deben considerar tanto el detalle como la validez de cada declaración de seguridad. Cuando realizan la evaluación de la seguridad y determinan la vulnerabilidad global de la cadena de suministro descrita en su Declaración de Aplicación.

Los socios que están cubiertos por el apartado 4.3 o por el apartado 4.4 no deberían necesitar ser evaluados más detenidamente.

Se debe documentar la siguiente información:

a) todos los escenarios de amenazas a la seguridad considerados;

b) los procesos utilizados al evaluar estas amenazas; y

c) todas las contramedidas identificadas y priorizadas.

5.4 Desarrollo del plan de seguridad de la cadena de suministro

Las organizaciones deben desarrollar y mantener un plan de seguridad para toda la parte de la cadena de suministro descrita en su Declaración de Aplicación. Se puede separar el plan en anexos en los que cada uno describa la seguridad establecida para un segmento particular de la cadena de suministro, incluyendo las medidas de seguridad que los socios de la organización, sujetos al apartado 4.3 o al apartado 4.4, mantendrán de acuerdo con sus declaraciones de seguridad. El plan o los anexos también deben especificar cómo la organización realizaría el seguimiento o revisaría periódicamente dichas declaraciones de seguridad.

Las organizaciones deben revisar y considerar el uso de la orientación en los anexos informativos A y B al desarrollar sus planes de seguridad.

5.5 Ejecución del plan de seguridad de la cadena de suministro

La organización debe establecer un sistema de gestión que permita que se implementen sus procesos de seguridad para la cadena de suministro.

5.6 Documentación y seguimiento de los procesos de seguridad para la cadena de suministro

5.6.1 Generalidades

La organización debe establecer y mantener procedimientos para documentar, hacer el seguimiento y medir el desempeño de su sistema de gestión anteriormente referido. La organización debe llevar a cabo auditorías del sistema de gestión a intervalos planificados para asegurarse de que se han implementado y se mantienen debidamente. Se deben documentar y conservar los resultados de las auditorías.

5.6.2 Mejora continua

La organización debe evaluar las oportunidades de mejorar sus disposiciones de seguridad como un modo de aumentar la seguridad de su parte de la cadena de suministro.

5.7 Acciones requeridas después de un incidente de seguridad

La organización debe llevar a cabo una revisión de su plan de seguridad después de que ocurra cualquier incidente de seguridad relativo a cualquier parte de la cadena de suministro internacional que la organización controla. Esta revisión debe:

a) determinar la causa del incidente y la acción correctiva;

b) determinar la eficacia de las medidas y los procedimientos para la recuperación de la seguridad; y

c) considerar tales resoluciones, volver a evaluar aquellas partes de la cadena de suministro de acuerdo con el apartado 5.3.2.

En caso de una brecha de la seguridad, la organización debe continuar informando de los procedimientos a Aduanas y/o a las autoridades adecuadas cuando sea apropiado, como se especifica en el plan de seguridad y en las relaciones contractuales.

La organización debe conservar el envío y otros datos de la cadena de suministro requeridos dentro de los tiempos límite prescritos en las leyes y los reglamentos aplicables.

5.8 Protección de la información de la seguridad

Se debe considerar a los planes, las medidas, los procesos, los procedimientos y los registros de seguridad como información reservada de la seguridad y se deben proteger del acceso o la revelación no autorizados. Dicha información sólo debe revelarse a individuos que tienen una "necesidad de saber". Además de los funcionarios de la autoridad apropiados o las personas por ellos designadas, un individuo tiene "necesidad de saber" cuando

a) el individuo requiere acceso a información reservada de la seguridad específica para llevar a cabo actividades de la seguridad cubiertas por el plan de seguridad;

b) el individuo se está formando para llevar a cabo actividades cubiertas por el plan de seguridad;

c) la información es necesaria para que el individuo supervise a otros que llevan a cabo actividades de la seguridad cubiertas por el plan de seguridad; o

d) el individuo es a quien, de acuerdo con una relación contractual con la organización, se le ha garantizado acceso a la información reservada de la seguridad controlada por la organización de acuerdo con los términos y condiciones acordados, o actúa en nombre de una parte.

NOTA Si se certifica que la organización cumple con la Norma ISO 28001 por medio de un organismo de certificación por tercera parte acreditado por un organismo de acreditación competente o se ha certificado o validado como cumplidor de la Norma ISO 28001 por gobiernos mutuamente reconocidos, dicho acceso a la información reservada de la organización acordado contractualmente puede no considerarse necesario, y en cualquier caso sería dependiente de la concurrencia explícita de la organización. El hecho de que su información reservada de la seguridad se proteja del acceso o la revelación no autorizados no evita que la organización informe a los socios u otros sobre sus acuerdos y sistemas de seguridad de la cadena de suministro.

ANEXO A (Informativo)

PROCESO DE SEGURIDAD DE LA CADENA DE SUMINISTRO

A.1 Generalidades

Este anexo proporciona una guía para el desarrollo de un proceso de seguridad de la cadena de suministro que se puede implementar en una organización que tenga un sistema de gestión. La figura A.1 proporciona una descripción gráfica de dicho proceso.

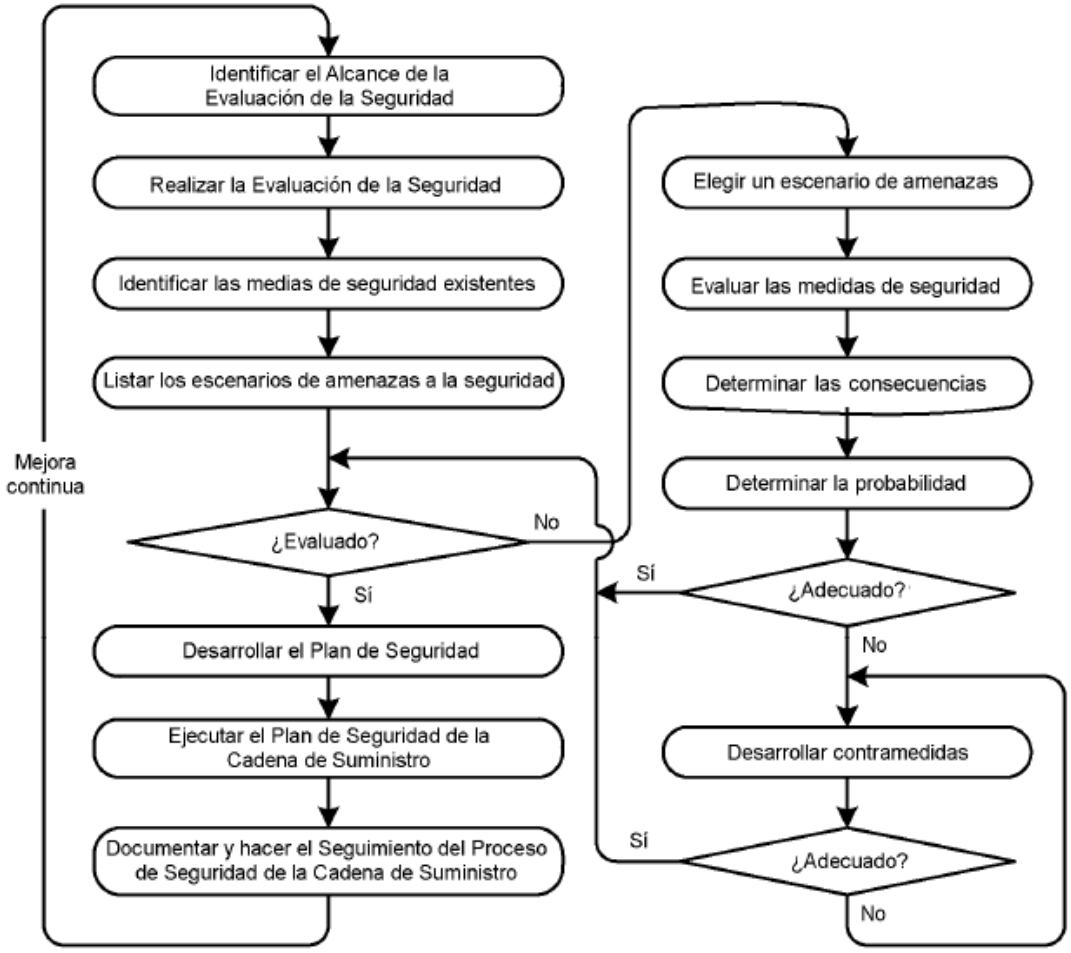

Figura A.1 – Descripción gráfica de un proceso de seguridad de la cadena de suministro

A.2 Identificación del alcance de la evaluación de la seguridad

Una evaluación de la seguridad es un intento de identificar los riesgos de la seguridad presentes en esa parte de la cadena de suministro que la organización, de acuerdo con su Declaración de Aplicación, desea que cumpla con esta norma internacional. Es necesario que se establezcan los límites del alcance de la cobertura (físicamente y virtualmente).

A.3 Realización de la evaluación de la seguridad

A.3.1 Generalidades

Los acuerdos de seguridad existentes en todos los emplazamientos tienen que evaluarse cuando hay cualquier potencial vulnerabilidad de la seguridad, utilizando personal cualificado lo que debería incluir, pero no limitarse a, lo siguiente:

- donde se fabrican, procesan o manipulan los bienes antes de ser cargados en una unidad de transporte, ser paletizados, o preparados de otro modo para enviarse;
- donde los bienes preparados para su envío se almacenan o se consolidan antes de su transporte;
- donde se transporten los bienes;
- donde los bienes se cargan o descargan después del transporte;
- donde la custodia de los bienes cambie de manos;
- donde se manipula, genera o es accesible la documentación o información relativa a los bienes transportados;
- las rutas de transporte interior utilizadas por los diversos medios de transporte;
- otro.

A.3.2 Lista de revisión del desempeño

La siguiente lista de revisión del desempeño proporciona un ejemplo de un enfoque sistemático para la revisión de acuerdos de seguridad existentes.

Aquellas partes de la lista de revisión del desempeño relativas a socios, que han confirmado a la organización que

a) se ha verificado que cumplen con esta norma internacional o con la Norma ISO 20858,

b) están cubiertos por el apartado 4.3, o

c) se les ha designado como OEA de acuerdo con el programa de seguridad de la cadena de suministro de una agencia nacional de aduanas, el cual se ha determinado que está de acuerdo con el marco de trabajo OMA SAFE,

deberían contener un comentario indicando cómo se ha tratado el factor, por ejemplo que cumple con esta norma internacional, con la Norma ISO 20858, o con el código ISPS.

A.3.3 Revisión del desempeño

La siguiente lista de revisión del desempeño que se muestra en la tabla A.1 puede completarse y considerarse cuando se realiza una evaluación de la seguridad para una organización en la cadena de suministro. Esta lista no es total, y puede ajustarse para reflejar la evaluación del riesgo y el modelo de negocio de la organización. Si la organización en la cadena de suministro ya implementa el factor indicado se debería marcar el bloque "Sí". Si el factor aún no se implementa o se cumple parcialmente se debería marcar el bloque "No" y, cuando sea aplicable, una explicación añadida a la columna de comentarios describiendo otras medidas alternativas utilizadas, o que el riesgo es muy bajo. Si el factor no es aplicable o está fuera de la declaración de cobertura de la organización, se debería anotar "No Aplicable" (NA) en el bloque "Comentarios". Los elementos de la lista de revisión del desempeño que no pueden desarrollarse debido a las leyes/reglamentos aplicables deberían marcarse como prohibidos en la columna de comentarios.

Tabla A.1 – Lista de revisión del desempeño

Factor	Sí	No	Comentarios
Gestión de la Seguridad de la Cadena de Suministro			
• ¿Tiene la organización un sistema de gestión que trata la seguridad de la cadena de suministro?			
• ¿Tiene la organización una persona designada como responsable para la seguridad de la cadena de suministro?			
Plan de Seguridad			
• ¿Tiene la organización uno o varios planes de seguridad establecidos?			
• ¿Trata el plan de las expectativas de seguridad de la organización de los socios aguas arriba y aguas abajo?			
• ¿Tiene la organización una gestión de crisis, una continuidad de negocio y un plan de recuperación de la seguridad?			
Seguridad de los Activos			
• ¿Tiene la organización establecidas medidas que traten – la seguridad física de los edificios, – el seguimiento y el control de los perímetros interior y exterior, – la aplicación de controles de acceso que prohíben el acceso no autorizado a las instalaciones, transportes, muelles de carga y áreas de carga, y control gerencial sobre la identificación (empleado, visitante, vendedor, etc.) y otros dispositivos de acceso? • ¿Hay tecnologías de seguridad operacional que aumenten significativamente la protección del activo? Por ejemplo, la detección de intrusos, o cámaras de grabación en CCTV/DVS que cubran las áreas de importancia para las actividades de la cadena de suministro, con los registros conservados un periodo de tiempo suficientemente largo como para ser de uso en la investigación de un incidente.			
• ¿Hay establecidos protocolos para contactar con el personal de seguridad interna o autoridades externas en caso de una brecha en la seguridad?			
• ¿Hay establecidos procedimientos para restringir, detectar e informar de accesos no autorizados a todas las áreas de carga y almacenaje de transporte?			
• ¿Se identifica a las personas que reparten o reciben carga antes de que la carga se reciba o se le dé salida?			
Personal de seguridad			
• ¿Tiene la organización procedimientos para evaluar la integridad de los empleados antes de la contratación y periódicas relativas a sus tareas de la seguridad?			
• ¿Lleva a cabo la organización una formación adecuada apropiada para un trabajo específico para asistir a los empleados al desarrollar sus tareas de la seguridad, por ejemplo: mantener la integridad de la carga, reconocer las potenciales amenazas internas a la seguridad y proteger los controles de acceso?			
• ¿Conciencia la organización a sus empleados sobre los procedimientos que tiene la compañía para informar de incidentes sospechosos?			

Factor	Sí	No	Comentarios
• ¿Incorpora el sistema de control del acceso la eliminación de la identificación de la compañía y el acceso a las áreas y sistemas de información reservada de los empleados despedidos?			
Seguridad de la información			
• ¿Se emplean procedimientos para asegurarse de que toda la información utilizada para el procesado de la carga, electrónico y manual, sea legible, oportuna, precisa, y está protegida contra alteración, pérdida o introducción de datos erróneos?			
• ¿Una organización que envía o recibe carga hace cuadrar la carga con la documentación de envío apropiada?			
• ¿Se asegura la organización de que se informa de modo preciso y oportuno de la información de la carga recibida de los socios?			
• ¿Se protegen los datos relevantes mediante el uso de sistemas de almacenaje no contingentes con la operación del sistema de manipulación de datos primarios (hay establecido un proceso de copias de seguridad)?			
• ¿Tienen todos los usuarios un identificador único (ID de usuario) para su uso personal y exclusivo, para asegurarse de que sus actividades pueden ser trazables hasta ellos?			
• ¿Se emplea un sistema de gestión de contraseñas eficaz para autentificar a los usuarios y se requiere que los usuarios cambien sus contraseñas al menos anualmente?			
• ¿Hay protección contra el acceso no autorizado y contra el mal uso de la información?			
Seguridad de los Bienes y el Transporte			
• ¿Están establecidos procedimientos para restringir, detectar, e informar del acceso no autorizado a todas las áreas de envío y muelles de carga y de almacenaje de las unidades de transporte de carga cerradas?			
• ¿Se han designado personas cualificadas para supervisar las operaciones de carga?			
• ¿Se han establecido procedimientos para notificar a las autoridades apropiadas el cumplimiento de la ley apropiado en casos en que la organización detecte o sospeche anomalías o actividades ilegales?			
• ¿Se han establecido procedimientos para asegurarse de la integridad de los bienes/la carga cuando los bienes/la carga se entregan a otra organización (proveedor de transporte, centro de consolidación, instalación intermodal, etc.) en la cadena de suministro?			
• ¿Se han establecido procesos para rastrear cambios en los niveles de amenaza a lo largo de las rutas de transporte?			
• ¿Hay reglas, procedimientos o guías de seguridad proporcionadas a las empresas de transporte (por ejemplo, el evitar rutas peligrosas)?			
Unidades de Transporte de Carga Cerradas			
(El marco de trabajo OMA SAFE incluye un "Programa de Integridad del Sello" descrito en el apéndice del anexo 1 que establece procedimientos con respecto a la fijación y verificación de sellos de alta seguridad y/u otros dispositivos de detección de manipulación. El personal que rellena este formulario debería revisar esa sección del Marco de Trabajo)			

Factor	Sí	No	Comentarios
• Si se utiliza una unidad de transporte de carga cerrada, ¿hay procedimientos documentados para la fijación y el registro de los sellos mecánicos de alta seguridad que cumplen el Documento ISO/PAS 17712 y/u otros dispositivos de detección de manipulación por la parte que carga la unidad de carga?			
• Si se utiliza una unidad de transporte de carga cerrada sellada, ¿hay establecidos procedimientos documentados para inspeccionar los sellos en busca de signos de manipulación cuando la custodia del transporte cambia en el curso de un envío y para tratar las discrepancias detectadas?			
• Si se utiliza una unidad de transporte de carga cerrada, ¿se inspecciona buscando contaminación por la parte que carga inmediatamente antes de la carga?			
• Si se utilizan unidades de transporte de carga cerradas, ¿se han establecido procedimientos documentados para inspeccionarlas inmediatamente antes de la carga por parte del que la carga para verificar su integridad física, para incluir la fiabilidad de los mecanismos de cierre de la unidad? Se recomienda un proceso de inspección de siete puntos: – Pared frontal – Lado izquierdo – Lado derecho – Suelo – Techo/Tejado – Cierre interior/exterior – Exterior/Tren de aterrizaje			

A.3.4 Escenarios de amenazas a la seguridad

Durante la evaluación de la seguridad se consideran escenarios de amenazas a la seguridad, incluyendo pero no limitándose a aquéllos que aparecen en la tabla A.2. La evaluación de la seguridad también debería considerar otros escenarios que pueden determinar las autoridades gubernamentales, la dirección de la organización o el profesional o profesionales de la seguridad que realizan la evaluación.

Tabla A.2 – Escenarios de amenazas a la seguridad de la cadena de suministro

Escenarios de amenazas a la seguridad	Aplicación
1 Introducir y/o tomar control de un activo (incluyendo transportes) en la cadena de suministro	Daño/destrucción de un activo (incluyendo transportes). Daño/destrucción de una meta exterior usando el activo o los bienes. Causar alteraciones civiles o económicas. Tomar rehenes/matar gente.
2 Usar la cadena de suministro como un medio de hacer contrabando	Armas ilegales entrando o saliendo del país/economía. Terroristas entrando o saliendo del país/economía.
3 Manipulación de la información	Conseguir el acceso local o remoto a la información/documentación de la cadena de suministro con el propósito de perturbar las operaciones o facilitar actividades ilegales.
4 Integridad de la carga	Manipulación, sabotaje y/o robo con fines terroristas.
5 Uso no autorizado	Realizar operaciones en la cadena de suministros internacional para facilitar un incidente terrorista incluyendo el uso del medio de transporte como un arma.
6 Otro	

A.4 Desarrollo del plan de seguridad

A.4.1 Generalidades

Se pueden incorporar el plan y/o los anexos de seguridad a los planes o procedimientos operacionales y no se necesita que sean documentos autónomos. Si el plan de seguridad se incorpora a otros planes la organización debería mantener una tabla de referencias cruzadas para permitir verificar que se han cumplido todos los requisitos del plan de seguridad.

Se puede separar el plan en anexos en los que cada uno describa la seguridad establecida para un segmento particular de la cadena de suministro, incluyendo las medidas de seguridad que los socios mantendrán de acuerdo con sus declaraciones de seguridad (si aplica). El plan o los anexos también debería especificar cómo la organización haría el seguimiento o revisaría periódicamente sus declaraciones de seguridad. El plan de seguridad o los anexos deberían incluir, pero no deberían limitarse a, descripciones de lo siguiente.

– La parte de la cadena de suministro que está cubierta por el plan o anexo.

– Las tareas relacionadas con la seguridad de todo el personal de seguridad.

– La estructura de gestión de la seguridad, incluyendo el nombre de la persona designada como director de seguridad.

– Información del contacto de seguridad interna y externa para que el personal la use al informar de un incidente de seguridad.

– Las habilidades y el conocimiento que requiera poseer el personal con responsabilidades en la seguridad.

– Los programas de formación en la seguridad.

– El proceso de cualificación para las personas a las que se han asignado tareas de la seguridad que asegure que se poseen las habilidades y el conocimiento necesarios para desarrollar sus tareas de la seguridad.

- Cómo se hace uso del plan de seguridad. Se puede usar la participación en los ejercicios de seguridad del gobierno o los ejercicios del personal de la organización para cumplir con estos requisitos.

- Procesos a cumplir, como un mínimo, requisitos de seguridad impuestos para contingencias por el gobierno o niveles de seguridad mayores.

El plan de seguridad debería contener procedimientos que incluyan, pero no se limiten a, los acuerdos que hacen lo siguiente.

- Asegurarse de que la información sobre un envío de bienes se recibe antes de que la organización acepte los bienes enviados para posterior transporte.

- Asegurarse de que los bienes o las cargas recibidas para consolidación/desconsolidación se hacen cuadrar con precisión con la información de los manifiestos/listas de los bienes o la carga. Las unidades de carga o de bienes de partida deberían verificarse con las órdenes de compra o entrega.

- Asegurarse de que los conductores que entregan o reciben los bienes o la carga están positivamente identificados antes de que las unidades de bienes o carga se reciban o se les dé salida.

- Asegurarse de que los ocupantes de los vehículos distintos a los conductores están positivamente identificados.

- Asegurarse, cuando sea necesario, de que toda falta, exceso, y otras discrepancias o anomalías significativas se resuelven y/o se investigan y que se notifica a las autoridades apropiadas si se detectan actividades ilegales o sospechosas.

- Describir cualquier contramedida que se haya implementado en esa parte de la cadena de suministro.

- Describir cualquier medida y procedimiento que se haya implementado en esa parte de la cadena de suministro para recuperar la seguridad cuando se produce un incidente de seguridad.

- Describir cualquier medida y procedimiento que se haya implementado cuando la custodia de los bienes o la carga se transfiere a otra organización.

- Describir los procedimientos para ceder información adicional sobre los bienes enviados al personal autorizado. Esto debería incluir cómo determinará el usuario si la demanda de información adicional es legítima y cómo y qué información se cede.

- Describir los procedimientos establecidos de acuerdo con el apartado A.4.3.

A.4.2 Documentación

La organización debería mantener la documentación más reciente de lo siguiente en un lugar de recuperación seguro.

- Declaraciones de cobertura.

- La evaluación de la seguridad completada.

- Nombres y cualificaciones del personal que realiza la evaluación de la seguridad.

- Listado de todas las contramedidas que se consideraron.

- Declaraciones de seguridad.

- Plan de seguridad y, si aplica, anexos.

– Registros de sesiones de formación y ejercicios realizados, personal que asistió, materias sobre las que se formó, y fecha(s).

– Otro según prescriban la reglamentación o la dirección.

A.4.3 Comunicación

Cuando sea viable, la organización debería establecer contacto con las autoridades apropiadas y otros funcionarios gubernamentales con los siguientes propósitos:

– Establecer procedimientos a seguir cuando se produce una sospecha de manipulación de los bienes o la carga, emergencias relacionadas con ello, o la recepción de amenazas que afectan a la cadena de suministro internacional. Si se dan, estos procedimientos deberían incluir números de teléfono específicos de las agencias gubernamentales apropiadas a los que llamar. Estos procedimientos se deberían incorporar al plan de seguridad de la cadena de suministro de la organización.

– Participar en las consultas dirigidas por funcionarios gubernamentales apropiados a niveles nacional y local (cuando sea apropiado) para discutir asuntos de interés mutuo incluyendo reglamentos y procedimientos de aduanas y requisitos para la seguridad local y del envío.

– Ser sensible a los esfuerzos de alcance del gobierno y contribuir al diálogo que proporciona una percepción significativa para asegurarse de que el plan de seguridad de la organización se mantiene de forma pertinente y eficaz.

Si la autoridad apropiada y otros funcionarios gubernamentales no desearan participar en dicho diálogo, la organización debería documentar su intento o intentos y establecer que el departamento de seguridad apropiado y otros funcionarios gubernamentales no participaron en esa ocasión.

A.5 Ejecución del plan de seguridad

La ejecución del plan de seguridad nuevo o revisado representa un cambio para las prácticas operacionales y necesita llevarse a cabo de acuerdo con el sistema de gestión de la organización para asegurarse de que están disponibles los recursos adecuados, se gestiona el impacto sobre otras operaciones y se hace el seguimiento y se evalúa la eficacia del plan.

A.6 Documentación y seguimiento del proceso de seguridad

La organización debería establecer y mantener procedimientos para hacer el seguimiento y medir el desempeño de su sistema de gestión de la seguridad para asegurarse de que continúa siendo indicado, adecuado y efectivo lo adecuado y eficacia. Cuando establece la frecuencia de medición y de seguimiento de los parámetros de desempeño clave, la organización debería considerar las amenazas y riesgos asociados a la seguridad, incluyendo el potencial deterioro de los mecanismos y sus consecuencias.

A.7 Mejora continua

La dirección del control operacional de esa parte de la cadena de suministro debería revisar el sistema de gestión de la seguridad de la organización para evaluar las oportunidades de mejora y la necesidad de cambios en el sistema de gestión de la seguridad.

ANEXO B (Informativo)

METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS DE LA SEGURIDAD Y EL DESARROLLO DE CONTRAMEDIDAS

B.1 Generalidades

Este anexo da una metodología que las organizaciones en cadenas de suministro internacionales pueden usar para hacer una evaluación del riesgo de incidentes de seguridad que podrían sufrir sus operaciones, para determinar las contra-medidas apropiadas, eficaces para el tipo y tamaño de sus operaciones en la cadena de suministro. Esta metodología utiliza la siguiente secuencia.

a) Listar todas las actividades comprendidas en el Objeto y campo de aplicación.

b) Identificar los controles de seguridad establecidos actualmente.

c) Identificar los escenarios de amenazas a la seguridad.

d) Determinar las consecuencias si se completó el escenario de amenazas a la seguridad.

e) Cuál es la probabilidad de que esto ocurra considerando la seguridad actual.

f) Si son adecuadas las medidas de seguridad.

g) Si no se desarrollan medidas de seguridad adicionales.

La figura B.1 es una representación gráfica de un proceso.

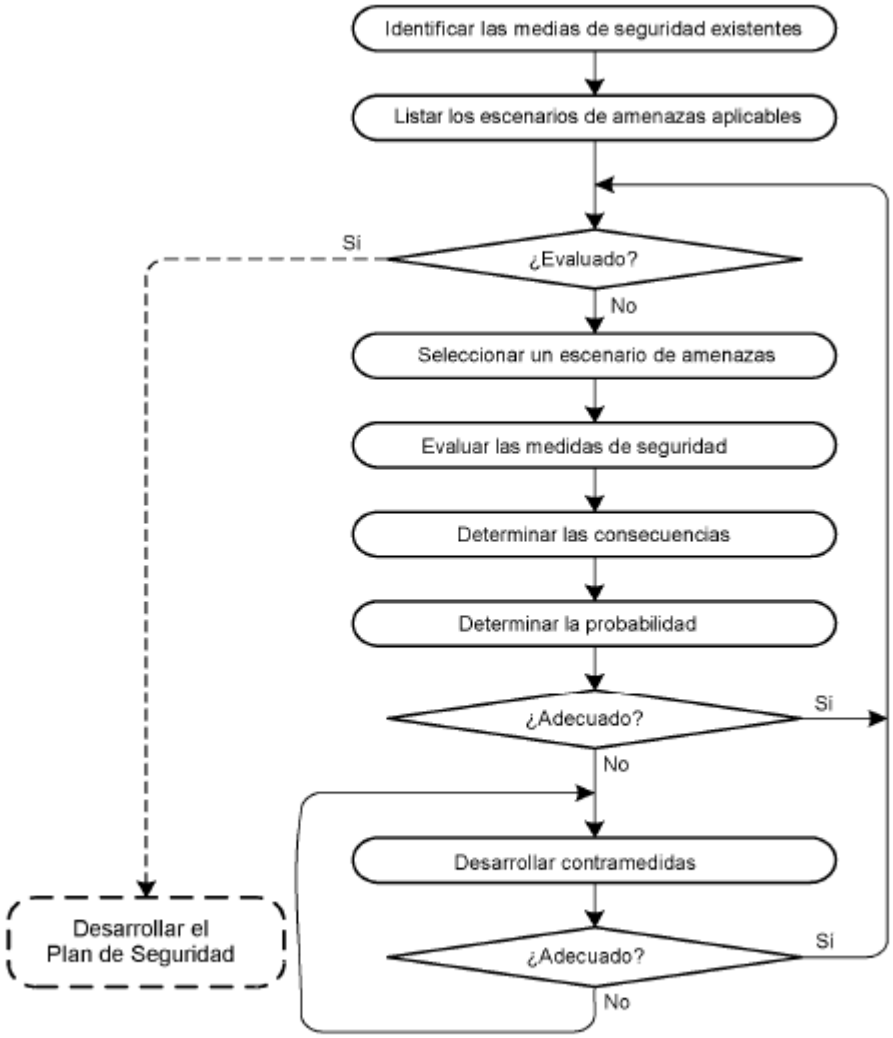

Figura B.1 – Representación gráfica de una metodología para la evaluación del riesgo de la seguridad

B.2 Paso uno – Consideración de los escenarios de amenazas a la seguridad

La evaluación de la seguridad debería considerar como mínimo los escenarios de amenazas a la seguridad que aparecen en la tabla B.1. La evaluación de la seguridad también debería considerar otros escenarios identificados por las autoridades gubernamentales, la dirección de la cadena de suministro o el profesional de la seguridad que realiza la evaluación.

Tabla B.1 – Escenarios de amenazas a la seguridad de la cadena de suministro

Escenarios de amenazas a la seguridad	Ejemplo de aplicación
1 Introducir y/o tomar control de un activo (incluyendo transportes) en la cadena de suministro	Daño/destrucción del activo (incluyendo transportes). Daño/destrucción de una meta exterior utilizando el activo o los bienes. Causar alteraciones civiles o económicas. Tomar rehenes/matar gente.
2 Usar la cadena de suministro como un medio de hacer contrabando	Armas ilegales entrando o saliendo del país/economía. Terroristas entrando o saliendo del país/economía.
3 Manipulación de la información	Conseguir el acceso local o remoto a la información/documentación de la cadena de suministro con el propósito de perturbar las operaciones o facilitar actividades ilegales.
4 Integridad de la carga	Manipulación, sabotaje y/o robo con fines terroristas.
5 Uso no autorizado	Realizar operaciones en la cadena de suministro internacional para facilitar un incidente terrorista (por ejemplo utilizando los medios de transporte como un arma).
6 Otro	

Durante la evaluación hay que considerar lo siguiente.

1) Control del acceso

   – en los locales de la organización en la cadena de suministro, incluyendo los alrededores;

   – en los medios de transporte (camión, ferrocarril, avión, barcaza, barco, etc.);

   – en la información;

   – otros.

2) Medios de transporte (camiones, ferrocarril, barcazas, aviones, barcos, etc.), teniendo en cuenta

   – operación normal;

   – talleres de mantenimiento (por ejemplo almacenes);

   – cambios debidos por ejemplo a averías;

   – cambio de medio;

   – medios de transportes en reposo;

   – utilización de medios de transporte como un arma;

   – otro.

3) Manipulación:
   - carga;
   - fabricación;
   - almacenaje (incluyendo almacenaje intermedio);
   - transferencia;
   - descarga;
   - desconsolidación/consolidación;
   - otro.
4) Transporte de bienes por
   - aire;
   - carretera;
   - ferrocarril;
   - aguas interiores;
   - aguas marítimas;
   - otro.
5) Detección/prevención de la intrusión aplicada a los envíos.
6) Inspecciones durante, por ejemplo la inspección de vehículos.
7) Empleados:
   - nivel de competencia, formación y toma de conciencia;
   - integridad;
   - otro.
8) Utilización de socios.
9) Comunicación interna/externa:
   - intercambio de información;
   - situaciones de emergencia;
   - otro.

10) Manipulación o procesado de la información sobre la carga o las rutas de transporte:

- protección de los datos;
- aseguramiento de los datos;
- otro.

11) Información externa:

- legal;
- órdenes de las autoridades;
- prácticas de la industria;
- accidentes e incidentes;
- capacidad de primera respuesta y tiempos de respuesta;
- otro.

B.3 Paso dos – Clasificación de las consecuencias

Una evaluación de las consecuencias debería considerar la pérdida de vidas y la pérdida económica potenciales. Las consecuencias de cada incidente de seguridad evaluado en la cadena de suministro deberían clasificarse como alto, medio o bajo (véase la tabla B.2). Se puede usar un sistema numérico en el proceso de evaluación, siempre que los resultados numéricos se conviertan a un sistema cualitativo.

Se deben documentar los racionales para la clasificación de las consecuencias para cada incidente de seguridad.

Se debería tener cuidado al establecer los valores de consecuencias "alto", "medio" y "bajo". El uso de umbrales de valores excesivamente bajos pueden resultar en el requisito de considerar contramedidas para más escenarios de amenazas a la seguridad de los necesarios. Sin embargo, el uso de umbrales de valores excesivamente altos puede omitir contramedidas para escenarios de amenazas a la seguridad que impliquen consecuencias que la organización o gobierno bajo el que se opera no puede tolerar.

Una clasificación de la consecuencia "alto" puede considerarse como una consecuencia que sería inaceptable en todas las situaciones salvo en las de probabilidad baja.

Una clasificación de la consecuencia "medio" puede considerarse como una consecuencia que sería inaceptable en una situación de probabilidad alta.

Una clasificación de la consecuencia "bajo" puede considerarse como una consecuencia que normalmente es aceptable.

La aceptabilidad no debería confundirse con la conveniencia o la aprobación. Más bien, la aceptabilidad podría considerarse como un juicio de la cantidad de daño posible que la organización o gobierno bajo el que se opera está dispuesto a aceptar bajo ciertas condiciones relacionadas con la probabilidad. Una organización o gobierno puede determinar que la posibilidad de un cierto nivel de daño puede ser no deseable pero sí aceptable.

Tabla B.2 – Clasificación de las consecuencias

Asignación de un valor	Consecuencia
Alto	**Fallecimiento y Lesiones** - pérdida de vidas a una cierta escala **y/o** **Impacto Económico** - daños mayores a un activo y/o infraestructura impidiendo operaciones posteriores **y/o** **Impacto Ambiental** - destrucción completa de múltiples aspectos del ecosistema de una gran área
Medio	**Fallecimiento y Lesiones** - por ejemplo pérdida de vidas **y/o** **Impacto Económico** - por ejemplo daños a un activo y/o infraestructura necesitando reparaciones **y/o** **Impacto Ambiental**- por ejemplo daños a largo plazo a una parte del ecosistema
Bajo	**Fallecimiento y Lesiones** - daños pero no pérdida de vidas **y/o** **Impacto Económico** - daños mínimos a un activo y/o infraestructura y sistemas **y/o** **Impacto Ambiental** - algún daño ambiental

B.4 Paso tres – Clasificación de la probabilidad de los incidentes de seguridad

Debería tenerse en cuenta, al clasificar los incidentes de seguridad potenciales, la categoría de las medidas de seguridad de la cadena de suministro, físicas y operacionales, tal como se han documentado en la lista de revisión del desempeño de la seguridad y en otra documentación proporcionada. Las medidas de seguridad físicas incluyen objetos que dificultan o detectan el acceso no autorizado a una meta. Las medidas de seguridad operacionales incluyen personas y procedimientos que dificultan o detectan el acceso no autorizado a una meta. Se debe clasificar la probabilidad de que ocurra cada incidente de seguridad como alta, media y baja.

- Debería utilizarse **probabilidad alta** cuando las medidas de seguridad establecidas ofrecen poca resistencia a que ocurra el incidente de seguridad. Si se utiliza un sistema numérico en el proceso de evaluación, los resultados numéricos deberían convertirse a este sistema cualitativo.

- Debería utilizarse **probabilidad media** cuando las medidas de seguridad establecidas ofrecen resistencia moderada a que ocurra el incidente de seguridad.

- Debería utilizarse **probabilidad baja** en casos en que las medidas de seguridad establecidas ofrezcan resistencia considerable a que ocurra el incidente de seguridad.

Se deberían documentar los racionales para la clasificación de la probabilidad asignada a cada incidente de seguridad.

B.5 Paso cuatro – Puntuación del incidente de seguridad

El diagrama de puntuación del incidente de seguridad dado en la tabla B.3 es un ejemplo que podría utilizarse para determinar cuándo deberían considerarse contramedidas para incidentes de seguridad específicos.

Tabla B.3 – Diagrama de puntuación del incidente de seguridad

		CLASIFICACIÓN DE LA PROBABILIDAD		
		Alta	**Media**	**Baja**
Clasificación de las consecuencias	**Alto**	**Contramedidas**	**Contramedidas**	**Considerar**
	Medio	**Contramedidas**	**Contramedidas o Considerar cuando sea apropiado**	**Documentar**
	Bajo	**Considerar**	**Documentar**	**Documentar**

Se requiere la identificación de contramedidas para los incidentes de seguridad que puntúen probabilidad y consecuencias alta, así como para aquéllos que puntúen probabilidad media y consecuencias alta. Otros incidentes de seguridad no necesitan incluir contramedidas, a menos que el evaluador lo considere aconsejable. La persona que evalúa la seguridad debería anotar cada incidente de seguridad que se requiera como para considerarse el uso de contramedidas.

NOTA La autoridad adecuada y otros funcionarios gubernamentales pueden especificar contramedidas para que se ejecuten ciertos escenarios de consecuencias extremadamente altas, a pesar de la probabilidad, como un asunto de política nacional. El gobierno que las requiere debería revisar la eficacia de las contramedidas desarrolladas como resultado de esta excepción.

B.6 Paso cinco – Desarrollo de contramedidas

Si se requiere o se considera aconsejable por el evaluador el desarrollo de una contramedida se deben considerar para su mitigación las consecuencias y/o la probabilidad. El objetivo es reducir la probabilidad de que un escenario de amenazas a la seguridad ocurra o reducir el daño que los escenarios de amenazas a la seguridad pueden causar a un nivel en el que ya no se requieran contramedidas adicionales.

Las contramedidas pueden producirse bajo las siguientes acciones.

– **Tratar**: pueden ser medidas de la organización y/o físicas.

– **Transferir**: la transferencia del riesgo puede ser la subcontrata, la transferencia física a otros lugares, tiempo, etc.

– **Terminar**: es posible que debido al nivel de riesgo la organización decida no continuar las actividades.

En ciertas circunstancias una organización puede tener que tolerar (véase la nota) un riesgo debido a lo poco práctico de las contramedidas necesarias, a la falta de autoridad para imponer las contramedidas necesarias u otros factores insalvables.

NOTA Tolerar la situación es que la organización no toma ninguna acción. Se deberían documentar y revisar periódicamente estas actividades y evaluaciones.

B.7 Paso seis – Implementación de las contramedidas

Las nuevas contramedidas representan un cambio en las prácticas operacionales y necesitan aprobarse de acuerdo con el sistema de gestión de la organización para asegurarse de que están disponibles los recursos adecuados, se gestiona el impacto sobre otras operaciones y el cambio tiene el apoyo de la dirección.

B.8 Paso siete – Evaluación de las contramedidas

Al utilizar los métodos especificados en esta norma internacional, se debería evaluar cada contramedida por su eficacia en disminuir la probabilidad o las consecuencias (o una combinación de ellas) hasta que el riesgo de la seguridad ya no requiera que se consideren medidas adicionales. Se considera que la contramedida que logra esto es eficaz, y debería añadirse al informe de evaluación de la seguridad.

B.9 Paso ocho – Repetición del proceso

Después de que las contramedidas se hayan desarrollado y se hayan evaluado como efectivas, se continúa el proceso con el siguiente escenario de amenazas a la seguridad hasta que el listado de escenarios se termine.

B.10 Continuación del proceso

El proceso de evaluación es continuo. Como ilustra la figura B.1, se debe hacer un seguimiento continuo de la seguridad para asegurarse de que las medidas de seguridad se desempeñan como se quería y el proceso de evaluación debería realizarse cuando sea necesario.

ANEXO C (Informativo)

ORIENTACIÓN PARA OBTENER CONSEJO Y CERTIFICACIÓN

C.1 Generalidades

No se obliga a las organizaciones que quieren implementar la Norma ISO 28001 a obtener los servicios de una consultora externa. Si una organización determina que necesita consejo o ayuda para: llevar a cabo la evaluación de la seguridad, el desarrollo de planes de seguridad, o la implementación de los requisitos necesarios, puede buscar servicios de consultoría externos. Sin embargo, es responsabilidad de la organización buscar consejo para comprobar y verificar la competencia de las consultoras que ofrecen servicios asesores, por ejemplo buscando recomendaciones, siguiendo referencias o revisando trabajos llevados a cabo. Los consultores que proporcionan servicios a la organización serían descartados para participar en auditorías por tercera parte a la misma organización.

C.2 Demostrar la conformidad con la Norma ISO 28001 mediante auditoría

La Norma ISO 28001 es una especificación de requisitos pensada para ayudar a organizaciones que optan voluntariamente por implementar los requisitos, establecer y demostrar un nivel apropiado de seguridad en aquellas partes de la cadena o cadenas de suministro internacional que controlan. Por tanto sirve como base para determinar, validar o demostrar el nivel de seguridad existente en las cadenas de suministro de las organizaciones a través de un proceso de auditoría por primera, segunda o tercera parte, o a través de una agencia gubernamental que escoja utilizar el cumplimiento con esta norma internacional como la base para la aceptación en sus programas de seguridad de la cadena de suministro.

Tipos de auditoría:

- Una auditoría por primera parte es la autodeterminación de la conformidad por la organización misma.
- Una auditoria por segunda parte es la determinación o verificación de la conformidad de una organización con criterios acordados por otra organización, agencia u organismo que tiene un interés creado en las operaciones de la organización en la cadena de suministro.
- Una auditoría por tercera parte es una determinación o verificación de la conformidad con criterios acordados a través de una organización independiente de todas las partes.

Validación y certificación a través del gobierno o agencia gubernamental.

Las agencias gubernamentales que eligen utilizar el cumplimiento con esta norma internacional como la base para la aceptación en sus programas de seguridad de la cadena de suministro pueden querer certificar y validar dicho cumplimiento ellos mismos o para evitar la duplicación pueden elegir delegar las auditorías a otras partes. La OMA establece unas guías para las administraciones de Aduanas relativas a los requisitos de validación y certificación para los programas de seguridad de la cadena de suministro de las Aduanas nacionales de acuerdo con el marco de trabajo OMA SAFE, y para el reconocimiento mutuo de dichos programas.

C.3 Certificación de la Norma ISO 28001 mediante organismos de certificación por tercera parte

Si se comprueba la demostración del cumplimiento a través de un proceso de auditoría por tercera parte, entonces la organización que busca la certificación debería considerar la selección de un organismo de certificación por tercera parte acreditado por un organismo de acreditación competente, tal como aquellos que son miembros del Foro Internacional de Acreditación (IAF) y sometido al Acuerdo de Reconocimiento Multilateral del IAF (MLA). Tales organismos de certificación acreditados cumplen con las reglas, códigos de práctica y protocolos de auditoría internacionalmente reconocidos, como la Norma ISO 17021 y la Norma ISO 19011. Véase la sección en las notas.

BIBLIOGRAFÍA

[1] ISO 9001:2000 *Sistemas de gestión de la calidad. Requisitos.*

[2] ISO 14001:2004 *Sistemas de gestión ambiental. Requisitos con orientación para su uso.*

[3] ISO 17021:2006 *Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.*

[4] ISO/PAS 17712:2006 *Contenedores de carga. Sellos mecánicos.*

[5] ISO 19011:2002 *Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental.*

[6] ISO 28000:2007 *Especificación para los sistemas de gestión de la seguridad para la cadena de suministro.*

[7] ISO 28003:2007 *Sistemas de gestión de la seguridad para la cadena de suministro. Requisitos para los organismos que realizan auditorías y certificación de los sistemas de gestión de la cadena de suministro.*

[8] *International Safety Management (ISM) Code, International Maritime Organization.*

[9] *SAFE Framework of Standards. Appendix to Annex 1, Word Customs Organization.*