NORMA CUBANA

NC

ISO 28000: 2010
(Publicada por la ISO en 2007)

ESPECIFICACIÓN PARA LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO (ISO 28000: 2007, IDT)

Specification for security management systems for the supply chain

ICS: 47.020.99

1. Edición Mayo 2010

Oficina Nacional de Normalización (NC) Calle E No. 261 Vedado, Ciudad de La Habana. Cuba. Teléfono: 830-0835 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 Organismo 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:

  - Dirección de Protección del Ministerio del Interior.
  - ACERPROT.
  - Ministerio de las Fuerzas Armadas Revolucionarias
  - Ministerio de la Informática y las Comunicaciones
  - SEPSA
  - IACC
  - Banco Central de Cuba
  - Oficina Nacional de Normalización.
  - AGESP.

- Es una adopción idéntica por el método de traducción de la Norma Internacional ISO 28000: 2007 *Specification for security management systems for the supply chain.*

Oficina Nacional de Normalización (NC)
Calle E No. 261, Vedado, Ciudad de La Habana, Habana 4, Cuba.

Impreso en Cuba.

0 Introducción

Esta Norma Internacional se ha desarrollado en respuesta a la demanda por parte de la industria de una norma sobre gestión de la seguridad. Su objetivo primordial es mejorar la seguridad de las cadenas de suministro. Es una norma de gestión de alto nivel que permite a una organización establecer un sistema de gestión global de la seguridad de las cadenas de suministro. Se requiere que la organización evalúe el entorno de seguridad en el que opera y que determine si se implementan unas medidas de seguridad adecuadas y si ya existen otros requisitos reglamentarios que la organización cumpla. Si mediante este proceso se identifican necesidades de seguridad, la organización debería implementar mecanismos y procesos para satisfacer estas necesidades. Puesto que las cadenas de suministro son de carácter dinámico, algunas organizaciones que gestionen múltiples cadenas de suministro pueden dirigirse a sus proveedores de servicios para satisfacer las normas gubernamentales o las normas ISO sobre seguridad de las cadenas de suministro como una condición para ser incluidos en esa cadena de suministro para simplificar la gestión de la seguridad como se ilustra en la Figura 1.

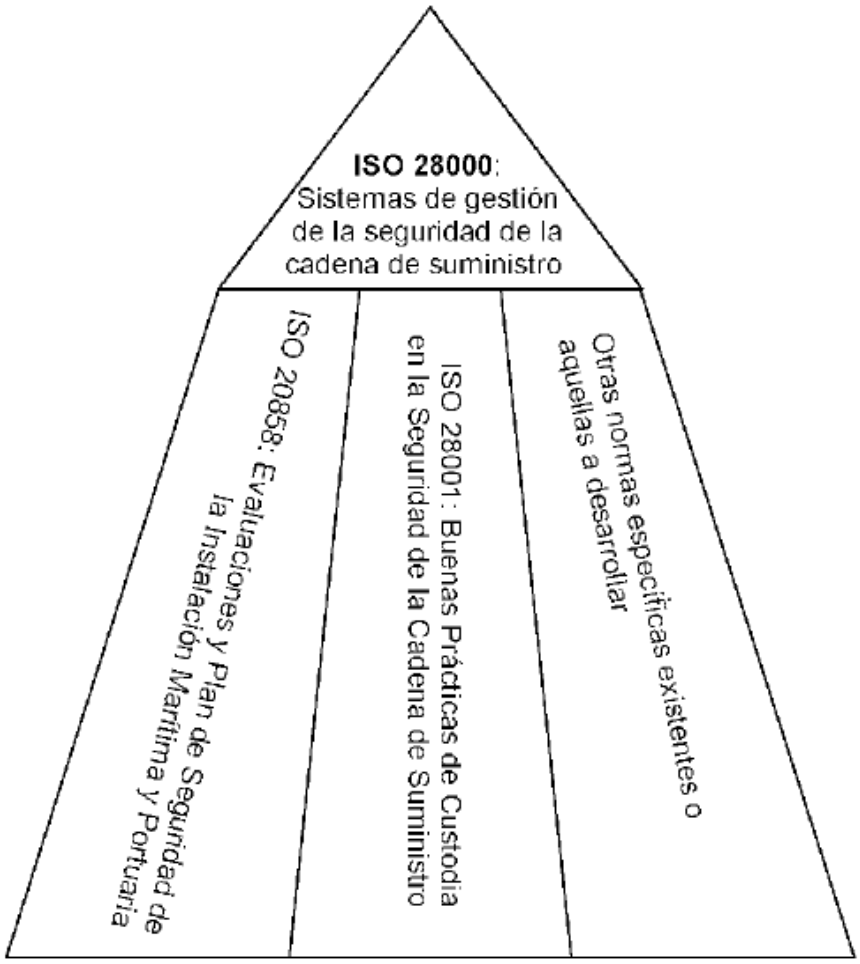

Figura 1 – Relación entre la Norma ISO 28000 y otras normas relevantes

Esta Norma Internacional está pensada para aplicarse en casos en los que se requiera que las cadenas de suministro de una organización se gestionen de manera segura. Un enfoque formal de la gestión de la seguridad puede contribuir directamente a la capacidad de negocio y a la credibilidad de organización.

El cumplimiento legal con una norma internacional no le confiere inmunidad respecto a las obligaciones legales. Para las organizaciones que pretendan tal cosa, el cumplimiento del sistema de gestión de la seguridad con esta Norma Internacional puede ser verificado mediante un proceso de auditoría externo o interno.

Esta Norma Internacional se basa en el formato ISO adoptado por la Norma 14001: 2004 por su enfoque de los sistemas de gestión basado en el riesgo. Sin embargo, las organizaciones que hayan adoptado un enfoque basado en procesos de los sistemas de gestión (por ejemplo, la Norma ISO 9001: 2000) pueden ser capaces de usar su sistema de gestión existente como base para un sistema de gestión de la seguridad como el prescrito en esta Norma Internacional. No es intención de esta Norma Internacional duplicar los requisitos gubernamentales y las normas relativas a la gestión de la seguridad de la cadena de suministro para los que la organización ya se haya certificado o se haya verificado que los cumple. La verificación puede ser por una primera, segunda o tercera parte aceptable.

NOTA: Esta Norma Internacional se basa en la metodología conocida como Planificar-Hacer-Verificar-Actuar (PHVA). La metodología PHVA se puede describir brevemente como sigue:

- Planificar: Establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con la política de seguridad de la organización.
- Hacer: Implementar los procesos.
- Verificar: Realizar el seguimiento y la medición de los procesos respecto a la política de seguridad, los objetivos, las metas, los requisitos legales y otros requisitos, e informar de los resultados.
- Actuar: Tomar acciones para mejorar continuamente el desempeño del sistema de gestión de la seguridad.

ESPECIFICACIÓN PARA LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

1 Objeto y campo de aplicación

Esta Norma Internacional especifica los requisitos para un sistema de gestión de la seguridad, incluyendo aquellos aspectos críticos para el aseguramiento de la seguridad de la cadena de suministro. La gestión de la seguridad está relacionada con muchos otros aspectos de la gestión del negocio. Estos aspectos incluyen todas las actividades controladas o influenciadas por organizaciones que tienen impacto sobre la seguridad de la cadena de suministro. Estos otros aspectos deberían considerarse directamente, donde y cuando tengan un impacto sobre la gestión de la seguridad, incluyendo el transporte de estos bienes a lo largo de la cadena de suministro.

Esta Norma Internacional se aplica a organizaciones de cualquier tamaño, desde pequeñas organizaciones a multinacionales, en la fabricación, el servicio, el almacenaje o el transporte en cualquier etapa de la cadena de producción o suministro que deseen:

a) establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad;

b) asegurar la conformidad con la política de gestión de la seguridad establecida;

c) demostrar dicha conformidad a otros;

d) buscar la certificación/registro de su sistema de gestión de la seguridad por un Organismo de Certificación por tercera parte Acreditado, o:

e) llevar a cabo una autodeterminación y una autodeclaración de conformidad con esta Norma Internacional.

Hay códigos legislativos y reglamentarios que tratan algunos de los requisitos de esta Norma Internacional.

Esta Norma Internacional no pretende requerir una demostración de la conformidad por duplicado.

Las organizaciones que escojan la certificación por tercera pate pueden demostrar mejor que contribuyen significativamente a la seguridad de la cadena de suministro.

2 Normas para consulta

No se citan normas para consulta. Este apartado se incluye con el propósito de mantener un orden numérico de los capítulos similar al de otras normas de sistemas de gestión.

3 Términos y definiciones

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

3.1 instalación

Instalaciones de planta, maquinaria, propiedad, edificios, vehículos, barcos o instalaciones portuarias, y otros elementos de la infraestructura o planta y sistemas relacionados que tengan una función o servicio de negocio definido y cuantificable.

NOTA Esta definición incluye cualquier código de software que sea crítico para la seguridad y la aplicación de la gestión de la seguridad.

3.2 seguridad
Resistencia al acto o actos intencionados y no autorizados destinados a causar daño o perjuicio a la cadena de suministro o a través de ella.

3.3 gestión de la seguridad
Actividades y prácticas sistemáticas y coordinadas a través de las cuales una organización gestiona de manera óptima sus riesgos y las amenazas e impactos potenciales asociados.

3.4 objetivo de la gestión de la seguridad
Resultado o logro específico requerido por la seguridad con el objeto de satisfacer la política de gestión de la seguridad.

NOTA Es esencial que dichos resultados estén relacionados directa o indirectamente con la provisión de los productos, el suministro o los servicios que entrega el negocio global a sus clientes o usuarios finales.

3.5 política de gestión de la seguridad
Intenciones y dirección globales de una organización, relacionadas con la seguridad y el marco de trabajo para el control de los procesos y actividades relacionados con la seguridad que se derivan de la política de la organización y los requisitos reglamentarios y que son consecuentes con ellos.

3.6 programas de gestión de la seguridad
Medios a través de los cuales se alcanza un objetivo de la gestión de la seguridad.

3.7 meta de la gestión de la seguridad
Nivel específico de desempeño requerido para alcanzar un objetivo de la gestión de la seguridad.

3.8 parte involucrada
Persona o entidad que tiene un derecho adquirido en el desempeño y el éxito de la organización o en el impacto de sus actividades.

NOTA Por ejemplo, clientes, accionistas, financieros, compañías aseguradoras, reguladores, entidades reglamentarias, empleados, contratistas, proveedores, organizaciones sindicales, o la sociedad.

3.9 cadena de suministro
Conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte.

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 que conducen al usuario final.

3.9.1 aguas abajo
Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro que ocurren después de que la carga abandone el control operacional directo de la organización, incluyendo, pero no limitándose, a los seguros, la financiación, la gestión de los datos, y al embalaje, almacenaje y transferencia de la carga.

3.9.2 aguas arriba
Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro que ocurren ante de que la carga esté bajo el control operacional directo de la organización, incluyendo, pero no limitándose, a los seguros, la financiación, la gestión de los datos, y al embalaje, almacenaje y transferencia de la carga.

3.10 alta dirección
Persona o grupo de personas que dirige y controla una organización al más alto nivel.

NOTA La alta dirección, especialmente en una multinacional grande, puede no estar implicada personalmente como se describe en esta Norma Internacional, sin embargo, se debe poner de manifiesto la responsabilidad de la alta dirección a través de la cadena de mando.

3.11 mejora continua
Proceso recurrente de optimización del sistema de gestión de la seguridad para lograr mejoras en el desempeño global de la seguridad de forma coherente con la política de seguridad de la organización.

4 Elementos del sistema de gestión de la seguridad

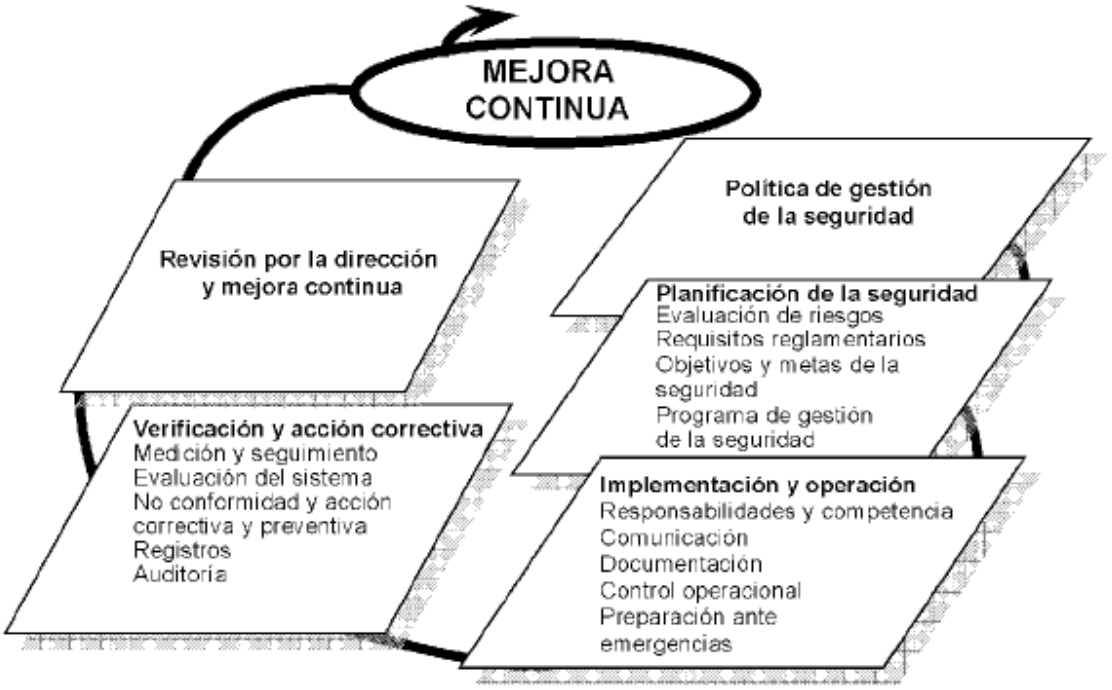

Figura 2 – Elementos del sistema de gestión de la seguridad

4.1 Requisitos generales

La organización debe establece, documentar, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad eficaz para identificar las amenazas a la seguridad, evaluar los riesgos y controlar y mitigar sus consecuencias.

La organización debe mejorar de manera continua su eficacia de acuerdo con los requisitos establecidos en todo el Capítulo 4.

La organización debe definir el alcance de su sistema de gestión de la seguridad. Cuando una organización escoge contratar externamente cualquier proceso que afecte a la conformidad con estos requisitos, la organización debe asegurar que dichos procesos se controlan. Se deben identificar dentro del sistema de gestión de la seguridad los controles y las responsabilidades necesarios de dichos procesos contratados externamente.

4.2 Política de la gestión de la seguridad

La alta dirección de la organización debe autorizar una política de gestión de la seguridad global. La política debe:

a) ser coherente con otras políticas de la organización;

b) proporcionar el marco de trabajo que permite que se produzcan los objetivos, las metas y los programas específicos de la gestión de la seguridad;

c) ser coherente con el marco de trabajo global de gestión de las amenazas y los riesgos de la seguridad;

d) ser apropiada a las amenazas a la organización y a la naturaleza y escala de sus operaciones;

e) establecer claramente los objetivos de la gestión de la seguridad globales/generales;

f) incluir un compromiso con la mejora continua del proceso de gestión de la seguridad;

g) incluir el compromiso de cumplir con la legislación aplicable en vigor, los requisitos legales y reglamentarios y con otros requisitos que la organización suscriba;

h) estar visiblemente refrendada por la alta dirección;

i) estar documentada, estar implementada y ser mantenida;

j) comunicarse a todos los empleados y terceras partes pertinentes, incluyendo contratistas y visitantes con la intención de que estas personas tomen conciencia de sus obligaciones individuales relativas a la gestión de la seguridad;

k) estar disponible para las partes afectadas cuando sea apropiado;

l) facilitar su revisión en caso de adquisición o fusión con otras organizaciones, u otro cambio en el alcance del negocio de la organización que pueda afectar a la continuidad o relevancia del sistema de gestión de la seguridad.

NOTA Las organizaciones pueden elegir tener una política de gestión de la seguridad detallada para uso interno que proporcionaría información y dirección suficientes para dirigir el sistema de gestión de la seguridad (algunas de cuyas partes pueden ser confidenciales) y tener una versión resumida (no confidencial) que contenga los objetivos generales para su difusión a las partes involucradas y otras partes interesadas.

4.3 Evaluación y planificación de los riesgos de la seguridad

4.3.1 Evaluación de los riesgos de la seguridad

La organización debe establecer y mantener procedimientos para la identificación y evaluación de las amenazas a la seguridad y de las amenazas y riesgos relativos a la gestión de la seguridad en curso, así como la identificación e implementación de las medidas de control de la gestión necesarias. Los métodos de identificación de las amenazas y riesgos, los métodos de evaluación y los métodos de control deberían, como mínimo, ser apropiados a la naturaleza y escala de las operaciones. Esta evaluación debe considerar la probabilidad de un evento y todas sus consecuencias, lo que debe incluir:

a) las amenazas y riesgos de fallo físico, tales como fallos funcionales, daños fortuitos, daños intencionales o acciones terroristas o criminales;

b) las amenazas y riesgos operacionales, incluyendo el control de la seguridad, los factores humanos y otras actividades que afecten al desempeño, la condición o la seguridad de la organización;

c) los sucesos naturales (tormentas, inundaciones, etc.), que pueden hacer que las medidas y los equipos de seguridad resulten ineficaces;

d) los factores ajenos al control de la organización, tales como fallos en el equipo y los servicios proporcionados externamente;

e) las amenazas y riesgos de las partes afectadas tales como el no cumplir con los requisitos reglamentarios o que se deteriore la reputación o la marca;

f) el diseño y la instalación del equipo de seguridad incluyendo los repuestos, el mantenimiento, etc.;

g) la gestión de información y datos y las comunicaciones;

h) una amenaza a la continuidad de las operaciones.

La organización debe asegurarse de que los resultados de estas evaluaciones y los efectos de estos controles se consideran y, cuando sea apropiado, proporcionan información de entrada para:

a) los objetivos y las metas de la gestión de la seguridad;

b) los programas de gestión de la seguridad;

c) la determinación de los requisitos para el diseño, la especificación y la instalación;

d) la identificación de los recursos adecuados, incluyendo el número de empleados;

e) la identificación de las necesidades de formación y las habilidades (véase el apartado 4.4.2);

f) el desarrollo de los controles operacionales (véase el apartado 4.4.6);

g) el marco de trabajo de la gestión de las amenazas y los riesgos globales de la organización.
La organización debe documentar y mantener la información anterior actualizada.

La metodología de la organización para la identificación y la evaluación de las amenazas y los riesgos debe:

a) definirse con respecto a su alcance, naturaleza y el momento en el tiempo para asegurarse de que es proactiva más que reactiva;

b) incluir la recopilación de la información relacionada con las amenazas y los riesgos a la seguridad;

c) proporcionar la clasificación de las amenazas y riesgos y la identificación de aquéllos que se tienen que evitar, eliminar o controlar;

d) proporcionar el seguimiento de las acciones para garantizar la eficacia y lo oportuno de su implementación (véase el apartado 4.5.1).

4.3.2 Requisitos legales y otros requisitos reglamentarios de la seguridad

La organización debe establecer, implementar y mantener un procedimiento

a) para identificar y tener acceso a los requisitos legales aplicables y a otros requisitos que la organización suscriba relacionados con sus amenazas y riesgos a la seguridad, y

b) para determinar cómo se aplican estos requisitos a sus amenazas y riesgos a la seguridad.

La organización debe mantener actualizada esta información. Debe comunicar la información pertinente sobre requisitos legales y otros requisitos a sus empleados y a otras terceras partes pertinentes, incluyendo a los contratistas.

4.3.3 Objetivos de la gestión de la seguridad

La organización debe establecer, implementar y mantener unos objetivos documentados sobre la gestión de la seguridad en las funciones y niveles pertinentes de la organización. Los objetivos deben derivarse de la política y ser coherentes con ella. Cuando establece y revisa sus objetivos, una organización debe tener en cuenta:

a) los requisitos legales y otros requisitos reglamentarios de la seguridad;

b) las amenazas y los riesgos relativos a la seguridad;

c) las opciones tecnológicas y de otro tipo;

d) los requisitos financieros, operacionales y de negocio;

e) las opiniones de las partes afectadas apropiadas;

Los objetivos de la gestión de la seguridad deben ser:

a) coherentes con el compromiso de mejora continua de la organización;
b) cuantificable (cuando sea viable);

c) comunicados a todos los empleados y a las terceras partes pertinentes, incluyendo a los contratistas, con el propósito de que estas personas tomen conciencia de sus obligaciones individuales;

d) revisados periódicamente para asegurarse de que siguen siendo pertinentes y coherentes con la política de gestión de la seguridad. Cuando sea necesario los objetivos de la gestión de la seguridad deben modificarse en consecuencia.

4.3.4 Metas de la gestión de la seguridad

La organización debe establecer, implementar y mantener metas de la gestión de la seguridad documentadas y apropiadas a las necesidades de la organización. Las metas deben derivarse de los objetivos de la gestión de la seguridad y ser coherentes con ellos.

Estas metas deben:

a) tener un nivel de detalle adecuado;

b) ser específicas, medibles, alcanzables, pertinentes y tener plazos (cuando sea viable);

c) comunicarse a todos los empleados y a las terceras partes pertinentes, incluyendo a los contratistas, con el propósito de que estas personas tomen conciencia de sus obligaciones individuales;

e) revisarse periódicamente para asegurarse de que siguen siendo pertinentes y coherentes con los objetivos de la gestión de la seguridad. Cuando sea necesario, las metas deben modificarse en consecuencia.

4.3.5 Programas de gestión de la seguridad

La organización debe establecer, implementar y mantener programas de gestión de la seguridad para alcanzar sus objetivos y metas.

Los programas deben optimizarse y entonces priorizarse, y la organización debe proporcionar los medios para la implementación eficiente y rentable de estos programas.

Esto debe incluir documentación que describa:

a) la responsabilidad y la autoridad designada para alcanzar los objetivos y las metas de la gestión de la seguridad;

b) los medios y la escala de tiempo por medio de los que se van a alcanzar los objetivos y las metas de la gestión de la seguridad.

Los programas de gestión de la seguridad deben revisarse periódicamente para asegurar que continúan siendo eficaces y coherentes con los objetivos y las metas. Cuando sea necesario los programas deben modificarse en consecuencia.

4.4 Implementación y operación

4.4.1 Estructura, autoridad y responsabilidades de la gestión de la seguridad

La organización debe establecer y mantener una estructura en la organización de funciones, responsabilidades y autoridad, coherente con el logro de su política, sus objetivos, sus metas y sus programas de gestión de la seguridad.

Estas funciones, responsabilidades y autoridad deben definirse, documentarse y comunicarse a las personas responsables de su implementación y su mantenimiento.

La alta dirección debe proporcionar evidencia de su compromiso con el desarrollo y la implementación del sistema de gestión de la seguridad (procesos) y de la mejora continua de su eficacia mediante:

a) la designación de un miembro de la alta dirección que, independientemente de otras responsabilidades, debe ser responsable del diseño, mantenimiento, documentación y mejora globales del sistema de gestión de la seguridad de la organización;

b) la designación de uno o varios miembros de la dirección con la autoridad necesaria para asegurar que se implementan los objetivos y las metas;

c) la identificación y el seguimiento de los requisitos y expectativas de las partes afectadas de la organización y la toma de la acción adecuada y oportuna para gestionar estas expectativas;

d) la garantía de disponibilidad de recursos suficientes;

e) la consideración del impacto adverso que la política de la gestión de la seguridad, los objetivos, las metas, los programas, etc. pueden tener sobre otros aspectos de la organización;

f) la garantía de que cualquier programa de seguridad generado por otras partes de la organización complementa el sistema de gestión de la seguridad;

g) la comunicación a la organización de la importancia de satisfacer sus requisitos de gestión de la seguridad para cumplir con su política;

h) la garantía de que las amenazas y los riesgos relativos a la seguridad se valoran y se incluyen en las evaluaciones de la organización de amenazas y riesgos, como corresponda;

i) la garantía de la viabilidad de los objetivos, las metas y los programas de gestión de la seguridad.

4.4.2 Competencia, formación y toma de conciencia

La organización debe asegurarse de que el personal responsable del diseño, la operación y la gestión del equipo y los procesos de seguridad están debidamente calificados en términos de educación, formación y/o experiencia. La organización debe establecer y mantener procedimientos para hacer que las personas que trabajen para ella o en su nombre sean conscientes de:

a) la importancia del cumplimiento con la política y los procedimientos de gestión de la seguridad, y con los requisitos del sistema de gestión de la seguridad;

b) sus funciones y responsabilidades en el logro del cumplimiento con la política y los procedimientos de gestión de la seguridad y con los requisitos del sistema de gestión de la seguridad, incluyendo los requisitos de preparación y respuesta ante emergencias;

c) las consecuencias potenciales para la seguridad de la organización de desviarse de los procedimientos operativos especificados.

Se deben guardar registros de la competencia y la formación.

4.4.3 Comunicación

La organización debe tener procedimientos para asegurar que se comunica a los empleados, contratistas y otras partes afectadas pertinentes y por ellos se recibe de ellos la información pertinente de la gestión de la seguridad.

Dada la naturaleza confidencial de cierta información relacionada con la seguridad, se debe tener la consideración debida a la confidencialidad de la información antes de la difusión.

4.4.4 Documentación

La organización debe establecer y mantener un sistema de documentación de la gestión de la seguridad que incluya aunque no se limite a, lo siguiente:

a) la política, los objetivos y las metas de la seguridad;

b) la descripción del alcance del sistema de gestión de la seguridad;

c) la descripción de los elementos principales del sistema de gestión de la seguridad y su interacción, y la referencia a los documentos relacionados;

d) los documentos, incluyendo los registros requeridos en esta Norma Internacional; y

e) los documentos, incluyendo los registros requeridos por la organización como necesarios para asegurar la eficacia de la planificación, operación y control de los procesos relacionados con sus amenazas y riesgos a la seguridad significativos.

La organización debe determinar la confidencialidad de la información y tomar medidas para evitar el acceso no autorizado.

4.4.5 Control de los documentos y los datos

La organización debe establecer y mantener procedimientos para controlar todos los documentos, datos e información requeridos en el Capítulo 4 de esta Norma Internacional para asegurar que:

a) estos documentos, datos e información están localizados y son accesibles sólo para las personas autorizadas;

b) estos documentos, datos e información se revisan periódicamente, se actualizan cuando sea necesario y se aprueban por personal autorizado;

c) las versiones en vigor de los documentos, datos e información pertinentes están disponibles en todos los puntos donde se lleven a cabo operaciones para el funcionamiento eficaz del sistema de gestión de la seguridad;

d) los documentos, datos e información obsoletos se eliminan sin demora de todos los puntos de expedición y de todos los puntos de uso, o se previene de otro modo su uso no intencionado;

e) los documentos, datos e información archivados, mantenidos con fines legales o de conservación de conocimientos o ambos, son fácilmente identificables;

f) estos documentos, datos e información son seguros, y si están en formato electrónico, se hacen las copias de seguridad apropiadas y pueden recuperarse.

4.4.6 Control operacional

La organización debe identificar aquellas operaciones y actividades que son necesarias para alcanzar:

a) su política de gestión de la seguridad;

b) el control de las actividades y la mitigación de las amenazas identificadas como de riesgo significativo;

c) el cumplimiento con los requisitos legales y otros requisitos reglamentarios de la seguridad;

d) sus objetivos de la gestión de la seguridad;

e) la difusión de sus programas de gestión de la seguridad;

f) el nivel requerido de seguridad en la cadena de suministro.

La organización debe asegurarse de que estas operaciones y actividades se llevan a cabo las condiciones especificadas mediante:

a) el establecimiento, la implementación y el mantenimiento de procedimientos documentados para controlar las situaciones en las que su ausencia podría llevar al fracaso en conseguir las operaciones y actividades relacionadas anteriormente en los puntos a) hasta f) de este apartado 4.4.6.

b) la evaluación de cualquier amenaza planteada por actividades aguas arriba en la cadena de suministro y la aplicación de controles para mitigar estos impactos en la organización y en otros operadores aguas debajo de la cadena de suministro;

c) el establecimiento y el mantenimiento de los requisitos para los bienes o servicios que tienen impacto en la seguridad y la comunicación de éstos a los proveedores y contratistas.

Cuando sea adecuado, estos procedimientos deben incluir los controles de diseño, instalación, operación, renovación y modificación de los elementos del equipo, instrumentos, etc., relativos a la seguridad. Cuando se revisen acuerdos existentes, o se introduzcan acuerdos nuevos, que pueden tener impacto en las operaciones y actividades de la gestión de la seguridad, la organización debe considerar las amenazas y riesgos asociados antes de su implementación. Los acuerdos nuevos o revisados a considerar deben incluir:

a) la estructura, las funciones o las responsabilidades de la organización revisadas;

b) la política, los objetivos, las metas o los programas de la gestión de la seguridad revisados;

c) los procesos y los procedimientos revisados;

d) la introducción de la nueva infraestructura, equipo o tecnología de seguridad, que puede incluir hardware y/o software;

e) cuando sea apropiado, la introducción de nuevos contratistas, proveedores o personal.

4.4.7 Reparación ante emergencias, respuesta y restablecimiento de la seguridad

La organización debe establecer, implementar y mantener planes y procedimientos adecuados para identificar los potenciales incidentes a la seguridad y las situaciones de emergencia, así como las respuestas a ellos, y evitar y mitigar las consecuencias probables que se les puede asociar. Los planes y procedimientos deben incluir la información sobre la provisión y el mantenimiento de cualquier equipo, instalación o servicios identificados que puedan requerirse durante los incidentes o situaciones de emergencia o tras ellos.

La organización debe revisar periódicamente la eficacia de sus planes y procedimientos de preparación, respuesta ante emergencias y de restablecimiento de la seguridad, en particular después de que ocurran incidentes o situaciones de emergencia causadas por violaciones y amenazas a la seguridad. Cuando sea factible la organización debe realizar pruebas periódicas de estos procedimientos.

4.5 Verificación y acción correctiva

4.5.1 Medición y seguimiento del desempeño de la seguridad

La organización debe establecer y mantener procedimientos para hacer el seguimiento y medir el desempeño de du sistema de gestión de la seguridad. También debe establecer y mantener procedimientos para hacer el seguimiento de los parámetros clave del desempeño, la organización debe considerar las amenazas y riesgos a la seguridad asociados, incluyendo el potencial deterioro de los mecanismos y sus consecuencias. Estos procedimientos deben asegurar:

a) las medidas cualitativas apropiadas a las necesidades de la organización;

b) el seguimiento del grado de cumplimiento de la política, los objetivos y las metas de la gestión de la seguridad;

c) las medidas del desempeño proactivas que realizan el seguimiento del cumplimiento con los programas de gestión de la seguridad, los criterios de control operacionales y los requisitos aplicables de legislación, reglamento y otros.
d) las medidas reactivas del desempeño para realizar el seguimiento de los deterioros, fallos, incidentes, no conformidades (incluyendo los cuasi-incidentes y las falsas alarmas) y otras evidencias históricas de un desempeño del sistema de gestión de la seguridad deficiente;

e) el registro de los datos y los resultados del seguimiento y la medición suficientes para facilitar las posteriores acciones de análisis correctivo y preventivo. Si se requiere un equipo de seguimiento para el desempeño y/o la medición y el seguimiento, la organización debe requerir el establecimiento y mantenimiento de los procedimientos para calibrar y mantener dicho equipo. Se deben conservar los registros de las actividades de calibración y mantenimiento el tiempo suficiente para cumplir con la legislación y la política de la organización.

4.5.2 Evaluación del sistema

La organización debe evaluar de manera periódica los planes, procedimientos y capacidades de gestión de la seguridad mediante revisiones, pruebas, informes posteriores a incidentes, lecciones aprendidas, evaluaciones del desempeño y ejercicios. Los cambios significativos en estos factores se deben reflejar inmediatamente en el procedimiento o procedimientos.

La organización debe evaluar periódicamente el cumplimiento con la legislación y los reglamentos pertinentes, las buenas prácticas de la industria y la conformidad con su propia política y objetivos.

La organización debe conservar los registros de los resultados de las evaluaciones periódicas.

4.5.3 Fallos, incidentes, no conformidades y acciones correctivas y preventivas relacionados con la seguridad

La organización debe establecer, implementar y mantener los procedimientos para definir la responsabilidad y autoridad para:

a) evaluar e iniciar las acciones preventivas para identificar fallos potenciales de la seguridad con el propósito de que pueda evitarse que ocurran;

b) la investigación de lo relativo a la seguridad:

   1) Los fallos incluyendo los cuasi-incidentes y las falsas alarmas;

   2) Los incidentes y las situaciones de emergencia;

   3) Las no conformidades;

c) la toma de acciones para mitigar cualquier consecuencia que surja de dichos fallos, incidentes y no conformidades;

d) el inicio y la finalización de las acciones correctivas;

e) la confirmación de la eficacia de las acciones correctivas tomadas.

Estos procedimientos deben requerir que se revisen todas las acciones correctivas y preventivas propuestas a través del proceso de evaluación de las amenazas y riesgos a la seguridad antes de la implementación, a menos que la implementación inmediata se anticipe a la exposición inminente de la seguridad humana o pública.

Cualquier acción correctiva o preventiva tomada para eliminar las causas de no conformidades reales y potenciales debe ser apropiada a la magnitud del problema y acorde con las amenazas y riesgos relativos a la gestión de la seguridad que se puedan encontrar. La organización debe implementar y registrar cualquier cambio en los procedimientos documentados como resultado de una acción correctiva y preventiva y, cuando sea necesario, se debe incluir la formación requerida.

4.5.4 Control de los registros

La organización debe establecer y mantener los registros que sean necesarios para demostrar la conformidad con los requisitos de su sistema de gestión de la seguridad y de esta Norma Internacional, y para demostrar los resultados logrados.

La organización debe establecer, implementar y mantener uno o varios procedimientos para la identificación, el almacenaje, la protección, la recuperación, el tiempo de retención y la disposición de los registros.

Los registros deben ser y conservarse legibles, identificables y trazables.

La documentación electrónica y digital debería ser a prueba de manipulaciones, con buenas copias de seguridad y accesible solamente para el personal autorizado.

4.5.5 Auditoría

La organización debe de establecer, implementar y mantener un programa de auditorías de la gestión de la seguridad y debe asegurarse de que las auditorías del sistema de gestión de la seguridad se llevan a cabo a intervalos planificados para:

a) determinar si el sistema de gestión de la seguridad:

   1) es conforme con los acuerdos planificados para la gestión de la seguridad, incluyendo los requisitos de todo el Capítulo 4 de esta especificación;

   2) se ha implementado y se mantiene adecuadamente;

   3) es eficaz para satisfacer la política y objetivos de la gestión de la seguridad de la organización;

b) revisar los resultados de las auditorías previas y de las acciones tomadas para rectificar las no conformidades;

c) proporcionar información de los resultados de las auditorías a la dirección;

d) verificar que el equipo y personal de seguridad se despliegan adecuadamente.

El programa de auditorías, incluyendo cualquier calendario, debe basarse en los resultados de las evaluaciones de las amenazas y riesgos de las actividades de la organización, y en los resultados de las auditorías previas. Los procedimientos de auditoría deben comprender el alcance, la frecuencia, las metodologías y las competencias, así como las responsabilidades y los requisitos para realizar auditorías e informar de los resultados. Cuando sea posible, las auditorías se deben realizar por personal independiente de aquél que tiene responsabilidades directas de la actividad examinada.

NOTA La frase “personal independiente” no significa necesariamente personal externo a la organización.

4.6 Revisión por la dirección y mejora continua

La alta dirección debe revisar el sistema de gestión de la seguridad de la organización, a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. Las revisiones deben incluir la evaluación de las oportunidades de mejora y la necesidad de efectuar cambios en el sistema de gestión de la seguridad, incluyendo la política de seguridad, los objetivos de la seguridad y las amenazas y riesgos. Se deben conservar los registros de las revisiones por la dirección. Los elementos de entrada para las revisiones por la dirección deben incluir

a) los resultados de las auditorías y evaluaciones del cumplimiento con los requisitos legales y otros requisitos que la organización suscriba;

b) las comunicaciones de las partes interesadas externas, incluyendo las quejas;

c) el desempeño de la seguridad de la organización;

d) el grado de cumplimiento de los objetivos y las metas;

e) el estado de las acciones correctivas y preventivas:

f) el seguimiento de las acciones resultantes de las revisiones previas llevadas a cabo por la dirección;

g) los cambios en las circunstancias, incluyendo la evolución de los requisitos legales y otros relacionados con su seguridad; y

h) las recomendaciones para la mejora.

Los resultados de las revisiones por la dirección, deben incluir todas las decisiones y acciones tomadas relacionadas con posibles cambios en la política, los objetivos y las metas de la seguridad y otros elementos del sistema de gestión de la seguridad, coherentes con el compromiso de mejora continua.

Anexo A
(informativo)

CORRESPONDENCIA ENTRE LA NORMA ISO 28000: 2007, LA NORMA ISO 14001: 2004 Y LA NORMA ISO 9001: 2000

ISO 28000: 2007		ISO 14001: 2004		ISO 9001: 2000	
Requisitos del sistema de gestión de la seguridad de la cadena de suministro (título solamente)	4	Requisitos del sistema de gestión ambiental (título solamente)	4	Requisitos del sistema de gestión de la calidad (título solamente)	4
Requisitos generales	4.1	Requisitos generales	4.1	Requisitos generales	4.1
Política de la gestión de la seguridad	4.2	Política ambiental	4.2	Compromiso de la dirección Política de la calidad Mejora continua	5.1 5.3 8.5.1
Evaluación y planificación de los riesgos de la seguridad (título solamente)	4.3	Planificación (título solamente)	4.3	Planificación (título solamente)	5.4
Evaluación de riesgos de la seguridad	4.3.1	Aspectos ambientales	4.3.1	Enfoque al cliente Determinación de los requisitos relacionados con el producto Revisión de los requisitos relacionados con el producto	5.2 7.2.1 7.2.2
Requisitos legales, reglamentarios y otros requisitos regulatorios de la seguridad	4.3.2	Requisitos legales y otros requisitos	4.3.2	Enfoque al cliente Determinación de los requisitos relacionados con el producto	5.2 7.2.1
Objetivos de la gestión de la seguridad	4.3.3	Objetivos, metas y programas	4.3.3	Objetivos de la calidad Planificación del sistema de gestión de la calidad Mejora continua	5.4.1 5.4.2 8.5.1
Metas de la gestión de la seguridad	4.3.4	Objetivos, metas y programas	4.3.3	Objetivos de la calidad Planificación del sistema de gestión de la calidad Mejora continua	5.4.1 5.4.2 8.5.1
Programas de la gestión de la seguridad	4.3.5	Objetivos, metas y programas	4.3.3	Objetivos de la calidad Planificación del sistema de gestión de la calidad Mejora continua	5.4.1 5.4.2 8.5.1
Implementación y operación (título solamente)	4.4	Implementación y operación (título solamente)	4.4	Realización del producto (título solamente)	7
Estructura, autoridad y responsabilidades de la gestión de la seguridad	4.4.1	Recursos, funciones, responsabilidad y autoridad	4.4.1	Compromiso de la dirección Responsabilidad y autoridad Representante de la dirección Provisión de recursos Infraestructura	5.1 5.5.1 5.5.2 6.1 6.3
Competencia, formación y toma de conciencia	4.4.2	Competencia, formación y toma de conciencia	4.4.2	(Recursos humanos) Generalidades Competencia, toma de conciencia y formación	6.2.1 6.2.2
Comunicación	4.4.3	Comunicación	4.4.3	Comunicación interna Comunicación con el cliente	5.5.3 7.2.3
Documentación	4.4.4	Documentación	4.4.4	(Requisitos de la documentación)Generalidades	4.2.1
Control de los documentos y los datos	4.4.5	Control de documentos	4.4.5	Control de los documentos	4.2.3
Control operacional	4.4.6	Control operacional	4.4.6	Planificación de la realización del producto	7.1

				Determinación de los requisitos relacionados con el producto	7.2.1
				Revisión de los requisitos relacionados con el producto	7.2.2
				Planificación del diseño y desarrollo	7.3.1
				Elementos de entrada para el diseño y desarrollo	7.3.2
				Resultados del diseño y desarrollo	7.3.3
				Revisión del diseño y desarrollo	7.3.4
				Verificación del diseño y desarrollo	7.3.5
				Validación del diseño y desarrollo	7.3.6
				Control de los cambios del diseño y desarrollo	7.3.7
				Proceso de compras	7.4.1
				Información de las compras	
				Verificación de los productos comprados	
				Control de la producción y de la prestación del servicio	7.5.1
				Validación de los procesos de la producción y de la prestación del servicio	7.5.2
				Preservación del producto	7.5.5
Preparación ante emergencias, respuesta y restablecimiento de la seguridad	4.4.7	Preparación y respuesta ante emergencias	4.4.7	Control del producto no conforme	8.3
Verificación y acción correctiva (título solamente)	4.5	Verificación (título solamente)	4.5	Medición, análisis y mejora (título solamente)	8
Medición y seguimiento del desempeño de la seguridad	4.5.1	Seguimiento y medición	4.5.1	Control de los dispositivos de seguimiento y medición	7.6
				Generalidades (medición, análisis y mejora)	8.1
				Seguimiento y medición de los procesos	8.2.3
				Seguimiento y medición del producto	8.2.4
				Análisis de datos	8.4
Evaluación del sistema	4.5.2	Evaluación del cumplimiento legal	4.5.2	Seguimiento y medición de los procesos	8.2.3
				Seguimiento y medición del producto	8.2.4
Fallos, incidentes, no conformidades y acciones correctivas y preventivas relacionadas con la seguridad	4.5.3	No conformidad, acción correctiva y acción preventiva	4.5.3	Control del producto no conforme	8.3
				Análisis de datos	8.4
				Acción correctiva	8.5.2
				Acción preventiva	8.5.3
Control de los registros	4.5.4	Control de los registros	4.5.4	Control de los registros	4.2.4
Auditoría	4.5.5	Auditoría interna	4.5.5	Auditoría interna	8.2.2
Revisión por la dirección y mejora continua	4.6	Revisión por la dirección	4.6	Compromiso de la dirección	5.1
				Revisión por la dirección (título solamente)	5.6
				Generalidades	5.6.1
				Información para la revisión	5.6.2
				Resultados de la revisión	5.6.3
				Mejora continua	8.5.1

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 19011: 2002 Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental.

[4] ISO/PAS 20858: 2004 Embarcaciones y tecnologías marinas. Evaluaciones de la seguridad de las instalaciones portuarias y desarrollo del plan de seguridad.

[5] ISO/PAS 28001 Sistema 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.

[6] ISO/PAS 28004: 2006 Sistemas de gestión de la seguridad para la cadena de suministro. Guía para la implementación de la Norma ISO 28000.