ESTANDAR INTERNACIONAL

ISO 28000

Especificación para sistemas de administración De seguridad para la cadena de suministro

Renuncia del PDF

Contenidos **página**

Prefacio

ISO (la organización internacional de estandarización) es una federación mundial de cuerpos estándar nacionales (cuerpos miembros de ISO). El trabajo de preparar estándares internacionales normalmente se lleva a cabo a través de comités técnicos de ISO. Cada cuerpo miembro interesado en un tema para el cual se ha establecido un comité técnico tiene el derecho de ser representado en ese comité. Organizaciones internacionales, gubernamentales y no gubernamentales, en alianza con ISO, también participan del trabajo. ISO colabora de cerca con la comisión electrotécnica internacional (IEC) en todos los temas de estandarización electrotécnica.

Se planean estándares internacionales de acuerdo con las reglas dadas en las directiva ISO/IEC, parte 2.

La tarea principal de los comités técnicos es preparar estándares internacionales. Los borradores de estándares internacionales adoptados por los comités técnicos se circulan a los miembros para su votación. Por ser un estándar internacional, su publicación requiere aprobación del por lo menos el 75% de los miembros poniendo en duda un voto.

Se presta atención en la posibilidad de que algunos de los elementos de este documento puedan ser tema de derecho patentado. ISO no será responsable por la identificación de todos ó algunos derechos patentados.

ISO 28000 fue preparado por el comité técnico ISO/TC 8, tecnología de barcos y marina en colaboración con otros comités técnicos relevantes responsables por asentimientos específicos de la cadena de abastecimiento.

Esta primera edición de ISO 28000 cancela y reemplaza a ISO/PAS 28000:2005, la cual ha sido técnicamente revisada.

Introducción

Este estándar internacional ha sido desarrollado como respuesta a demanda de la industria para un estándar de administración de seguridad. Su objetivo principal es mejorar la cadena de abastecimiento de seguridad. Es un estándar administrativo de alto nivel que permite a una organización establecer un sistema de administración de seguridad de cadena de abastecimiento general. Requiere que la organización valore el ambiente de seguridad en el que opera y para determinar si las medidas de seguridad adecuadas están en su sitio y si ya existen otros requerimientos reguladores con los que cumpla la organización. Si por este proceso se identifican necesidades de seguridad, la organización debe implementar mecanismos y procesos
Para satisfacer estas necesidades. Ya que las cadenas de abastecimiento son dinámicas por naturaleza, algunas organizaciones que manejan cadenas de abastecimiento múltiples, pueden mirar a sus proveedores de servicios para alcanzar estándares relacionados con el gobierno ó cadena de abastecimiento de ISO como una condición para ser incluido en esa cadena de abastecimiento para simplificar la administración de seguridad como se ilustra en la figura 1.

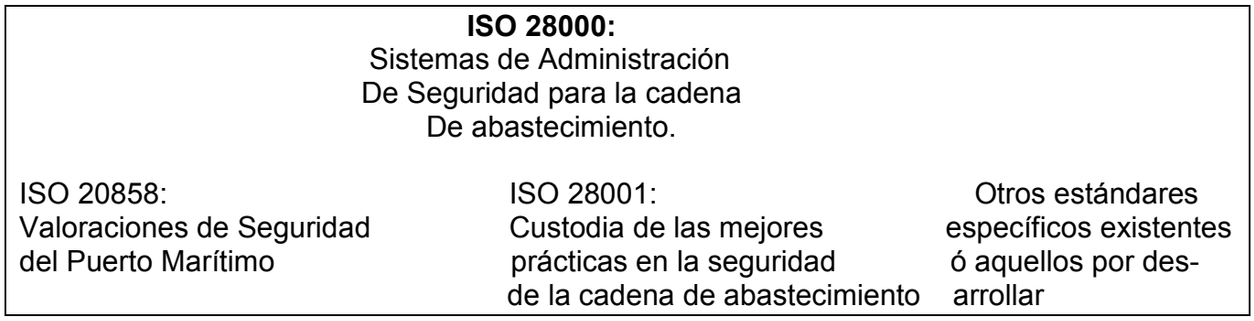

Figura 1: Relación entre ISO 28000 y otros estándares relevantes

Este estándar internacional está intencionado para aplicar en casos donde las cadenas de abastecimiento de una organización, tengan que ser manejadas de forma segura. Un acercamiento formal a administración de seguridad puede contribuir directamente con la capacidad del negocio y credibilidad de la organización.

El cumplimiento con un estándar internacional no lleva en sí mismo inmunidad de las obligaciones legales. Para las organizaciones que así lo quieran, el cumplimiento con el sistema de administración de seguridad con este estándar internacional puede ser verificado por un proceso de auditoria externa ó interna.

Este estándar internacional está basado en el formato ISO adoptado por ISO 14001:2004 debido a su riesgo basado en el acercamiento a sistemas administrativos. Sin embargo, organizaciones que han adoptado un proceso de acercamiento a los sistemas administrativos (e.g. ISO 9001:2000) podrán utilizar su sistema de administración de seguridad actual como la base para un sistema de administración de seguridad como se prescribe en este estándar internacional. No es la intención de este estándar internacional, el duplicar los requerimientos gubernamentales y estándares con respecto a la administración de seguridad de la cadena de abastecimiento, por la cual la organización ya ha sido certificada ó se ha verificado cumplimiento. La verificación se puede llevar a cabo por un grupo organizacional inicial, secundario o tercero.

NOTA: Este estándar internacional se basa en la metodología conocida como Plan-Hacer-Revisar-Actuar (PDCA). PDCA puede ser descrito de la siguiente manera:

- Plan: Establecer los objetivos y procesos necesarios para obtener resultados acordes con la política de seguridad de la organización.
- Hacer: Implementar el Proceso.
- Revisar: Monitorear y medir procesos
- Actuar: Tomar acciones para mejorar continuamente el funcionamiento del sistema de administración de seguridad.

Especificación para sistemas de administración de seguridad para la cadena de abastecimiento

1 Alcance

Este estándar internacional especifica los requerimientos para un sistema de administración de seguridad, incluyendo aquellos aspectos críticos para garantizar la seguridad de la cadena de abastecimiento. Aspectos incluyen todas las actividades controladas ó influenciadas por organizaciones que impactan en la seguridad de la cadena de abastecimiento. Estos otros aspectos deberían ser considerados directamente, dónde y cuándo éstos tienen un impacto en el manejo de seguridad, incluyendo el transporte de estos bienes a lo largo de la cadena de abastecimiento.

Este Estándar Internacional es aplicable a todos los tamaños de organizaciones, de pequeñas a multinacionales, en manufactura, servicios, almacenamiento ó transporte en cualquier etapa de la cadena de producción ó de abastecimiento que tenga la intención de:

a) Establecer, implementar, mantener y mejorar un sistema de manejo de seguridad.

b) Asegurar conformidad con la política de administración de seguridad establecida.

c) Demostrar dicha conformidad a otros.

d) Buscar certificación/registro de su sistema de manejo de seguridad por parte de un tercero acreditado.

e) Hacer una determinación y declaración propia de conformidad con este Estándar Internacional.

No es la intención de este Estándar Internacional exigir demostración duplicada de conformidad.

Las organizaciones que elijan certificación de un tercero, pueden demostrar más adelante que están contribuyendo significativamente con la seguridad de la cadena de abastecimiento.

2 Referencias Normativas

No hay referencias normativas citadas. Esta cláusula está incluida para retener una numeración de cláusulas similar al de otros estándares de sistemas administrativos.

3 Términos y Definiciones

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

3.1
Facilidad
Planta, maquinaria, propiedad, edificios, vehículos, barcos, instalaciones del puerto y otros elementos de infraestructura ó planta y sistemas relacionados, que tienen una función de negocios distintiva y cuantificable ó servicios.

NOTA
Esta definición incluye cualquier código de software que sea crítico para el envío de seguridad y la aplicación de administración de la misma.

3.2
Seguridad
Resistencia a actos intencionales, no autorizados diseñados para causar daño a ó por la cadena de abastecimiento.

3.3
Administración de Seguridad
Actividades sistemáticas y coordinadas y prácticas a través de las cuales una organización maneja de manera óptima sus riesgos y las amenazas potenciales asociadas e impactos dados.

3.4
Objetivos de la Administración de Seguridad
Resultado específico ó logro de seguridad requerido para cumplir con la política de manejo de seguridad.

3.5
Política de la Administración de Seguridad
Intenciones generales y dirección de una organización, relacionada con la seguridad y estructura para el control de procesos y actividades relacionados con seguridad que se derivan de y son consistentes con la política de la organización y requisitos reguladores.

3.6
Programas de administración de seguridad
Son los medios mediante los cuales se logra un objetivo de manejo de seguridad.

3.7
Target del Manejo de Seguridad
Nivel específico de funcionamiento requerido para lograr un objetivo de la administración de seguridad.

3.8
Tenedor de Apuestas
Persona ó entidad con un interés invertido en el funcionamiento de la organización, éxito ó impacto de estas actividades.

NOTA Ejemplos incluyen clientes, accionistas, financieros, aseguradores, reguladores, cuerpos reglamentarios, empleados, contratantes, proveedores, organizaciones laborales ó sociedad.

3.9
Cadena de Abastecimiento
Grupo relacionado de fuentes y procesos que comienza con el nacimiento de materia prima y se extiende hacia el envío de productos ó servicios al usuario final a través de los medios de transporte.

NOTA La cadena de abastecimiento puede incluir vendedores, instalaciones de manufacturación, proveedores de logística, centros de distribución interna, distribuidores, mayoristas y otras entidades que llevan al usuario final.

3.9.1
Río abajo
Se refiere a las acciones, procesos y movimientos de la carga dentro de la cadena de abastecimiento que ocurren después de que la carga deja el control directo operacional de la organización, incluyendo pero no limitado al seguro, finanzas, administración de información y el empaque, almacenamiento y transferencia de la carga.

3.9.2
Ría arriba
Se refiere a las acciones, procesos y movimientos de la carga dentro de la cadena de abastecimiento que vienen por debajo de la carga que deja el control directo operacional de la organización, incluyendo pero no limitado al seguro, finanzas, administración de información y el empaque, almacenamiento y transferencia de la carga.

3.10
Administración Superior
Es la persona ó grupo de personas que dirigen y controlan una organización en el más alto nivel.

NOTA: La administración superior, especialmente en una organización multinacional grande, puede no estar personalmente involucrado como se menciona en este estándar internacional: sin embargo la responsabilidad de la administración superior a través de la cadena de comando será manifestada.

3.11
Mejoramiento Continuo
Proceso recurrente de aumentar el sistema del manejo de seguridad, para lograr mejoramientos en el funcionamiento general de seguridad, consistente con la política de seguridad de la organización.

4. Elementos del Sistema del Manejo de Seguridad

MEJORAMIENTO CONTINUO

Revisión de Manejo **Política de Manejo de Seguridad**

Acción Correctiva y de Chequeo
Medición y monitoreo
Evaluación del sistema
No-conformidad y acción correctiva
Y preventiva
Registros
Auditoria

Planeación de Seguridad
Valoración del Riesgo
Comunicación
Documentación
Control Operativo
Preparación para emergencias

Figura 2 – Elementos del Sistema de Administración de Seguridad

41. Requerimientos Generales

La organización establecerá, documentará, implementará, mantendrá y mejorará continuamente un sistema de manejo de seguridad eficiente para identificar amenazas de seguridad, valorar riesgos y controlar y mitigar sus consecuencias.

La organización mejorará continuamente su efectividad de acuerdo con los requerimientos expuestos en toda la cláusula 4.

La organización definirá el alcance de su sistema de administración de seguridad. Donde una organización elija subcontratar cualquier proceso que afecte la conformidad con estos requerimientos, la organización se asegurará de que dichos procesos sean controlados. Los controles necesarios y responsabilidades de dichos procesos subcontratados serán identificados dentro del sistema de manejo de seguridad.

4.2 Política de Administración de Seguridad

La administración de alto nivel de la organización autorizará una política de manejo de seguridad. La política:

a) será consistente con otras políticas organizacionales;

b) Proveerá la estructura que permita los objetivos específicos de manejo de seguridad, targets y programas a ser producidos;

c) Ser consistente con la amenaza general de seguridad de la organización y estructura de riesgo de la administración.

d) Ser apropiada con las amenazas de la organización y la naturaleza y escala de sus operaciones.

e) Afirmar claramente los objetivos generales del manejo de seguridad.

f) Incluir un compromiso de mejoramiento continuo del proceso de manejo de administración.

g) Incluir un compromiso de cumplir con la legislación aplicable actual, requerimientos reguladores y reglamentarios y con otros requerimientos con los que se suscribe la organización.

h) Ser endosada visiblemente por la administración superior.

i) Ser documentada, implementada y mantenida.

j) Ser comunicada a todos los empleados relevantes y terceros incluyendo contratistas y visitantes con la intención de que estas personas sean advertidas sobre sus obligaciones individuales relacionadas con el manejo de seguridad.

k) Estar disponible para los tenedores de apuestas donde sea apropiado.

l) Proveer para su revisión, en caso de la adquisición de, ó fusión con otras organizaciones, u otro cambio en el alcance del negocio de la organización que pueda afectar la continuidad ó relevancia del sistema de manejo de seguridad.

NOTA Las organizaciones pueden escoger entre tener una política detallada del manejo de seguridad para uso interno que podría proveer suficiente información y dirección para manejar el sistema de manejo de seguridad (partes que pueden ser confidenciales) ó de tener una versión resumida (no – confidencial) que contenga los objetivos generales para la diseminación para sus tenedores de apuestas y otras partes interesadas.

4.3 Valoración del Riesgo de Seguridad y Planeación

4.3.1 Valoración del riesgo de seguridad

La organización establecerá y mantendrá procedimientos para la identificación continua y valoración de las amenazas de seguridad y amenazas relacionadas con el manejo de seguridad y riesgos, y la identificación e implementación de medidas de control administrativas necesarias. Amenazas de seguridad y riesgo de identificación, valoración y métodos de control deberían, como mínimo, ser apropiadas a la naturaleza y escala de las operaciones. Esta valoración considerará la probabilidad de un evento y de todas sus consecuencias que incluirá:

a) Amenazas y riesgos de fallas físicas, como pérdida funcional, daño incidental, daño malicioso, terrorista ó acción criminal;

b) Amenazas y riesgos operativos, incluyendo el control de la seguridad, factores humanos y otras actividades que afectan el funcionamiento, condición o seguridad de la organización.

c) Eventos ambientales naturales (tormenta, inundación, etc.), que pueden inutilizar las medidas de seguridad y equipos no efectivos.

d) Factores ajenos al control de la organización, como fallas en equipos suministrados externamente y servicios;

e) Amenazas y riesgos del tenedor de apuestas como fallas para cumplir con los requerimientos reguladores o daño a la reputación ó marca;

f) Diseño e instalación de equipo de seguridad incluyendo reemplazo mantenimiento, etc.

g) Información y administración de datos y comunicaciones;

h) Una amenaza a la continuidad de las operaciones.

La organización se asegurará que los resultados de estas valoraciones y los efectos de estos controles se consideren y, donde sea apropiado, proveer inversión en:

a) Objetivos y metas de la administración de seguridad;

b) Programas de administración de seguridad;

c) La determinación de requisitos para el diseño, especificación e instalación;

d) Identificación de recursos adecuados incluyendo niveles de personal;

e) Identificación de necesidades de entrenamiento y habilidades (ver 4.4.2);

f) Desarrollo de controles operativos (ver 4.4.6);

g) La amenaza general de la organización y estructura de manejo de riesgos;

La organización documentará y mantendrá la información anterior actualizada.
La metodología de la organización para identificación de amenaza y riesgo y valoración deberá:

a) ser definida con respecto a su enfoque, naturaleza y tiempo para asegurar su pro activo en lugar de su reactivo;

b) Incluir la recolección de información relacionada con amenazas y riesgos de seguridad;

c) Proveer para la clasificación de amenazas y riesgos e identificación de los que deben ser evadidos, eliminados ó controlados;

d) Proveer para el monitoreo de acciones para asegurar efectividad y la falta de tiempo de su implementación (ver 4.5.1).

4.3.2 Requerimientos legales y reguladores de seguridad

La organización establecerá, implementará y mantendrá a procedimiento

a) identificar y tener acceso a los requerimientos legales aplicables y otros requerimientos a los que se suscribe la organización relacionados con la amenaza y riesgos de seguridad y

b) determinar como estos requerimientos aplican a sus amenazas y riesgos de seguridad.

La organización mantendrá esta información actualizada. Comunicará información relevante al aspecto legal y otros requerimientos a sus empleados y otras terceras partes relevantes incluyendo contratistas.

4.3.3 Objetivos del Manejo de Seguridad

La organización establecerá, implementará y mantendrá documentados los objetivos del manejo de seguridad a funciones y niveles relevantes dentro de la organización. Los objetivos serán derivados de y consistentes con la política. Al establecer y revisar sus objetivos, la organización tendrá en cuenta:

a) Requerimientos legales y reguladores de seguridad;

b) Amenazas y riesgos relacionados con seguridad;

c) tecnológicos y otras opciones;

d) Requerimientos financieros, operativos y de negocios;

e) Puntos de vista de tenedores de apuestas importantes.

Los objetivos de la administración de seguridad serán:

a) Consistentes con el compromiso de la organización del mejoramiento continuo;

b) Cuantificado (donde aplique);

c) Comunicados a todos los empleados relevantes y terceros, incluyendo contratistas, con la intención que estas personas estén al tanto de sus obligaciones individuales;

d) Revisados periódicamente para asegurar que se mantengan relevantes y consistentes con la política de administración de seguridad. Donde sea necesario, los objetivos del manejo de seguridad serán enmendados.

4.3.4 Metas del Manejo de Seguridad

La organización establecerá, mantendrá e implementará metas documentadas del manejo de seguridad apropiadas a las necesidades de la organización. Las metas serán derivadas de y serán consistentes con los objetivos de la administración de seguridad.

Estas metas serán:

a) a un nivel de detalle apropiado;

b) específicas, relevantes, alcanzables y basadas en tiempo (donde aplique);

c) Comunicadas a todos los empleados relevantes y terceros incluyendo contratistas con la intención de que estas personas estén conscientes de sus obligaciones individuales;

d) Revisadas periódicamente para asegurar que se mantengan relevantes y consistentes con la política de administración de seguridad. Donde sea necesario, las metas del manejo de seguridad serán enmendados.

4.3.5 Programas del Manejo de Seguridad

La organización establecerá, mantendrá e implementará programas del manejo de seguridad para lograr sus objetivos y metas.

Estos programas serán optimizados y luego priorizados, y la organización proveerá para la implementación eficiente y costo eficiente de estos programas.

Esto incluirá documentación que describe:

a) La responsabilidad designada y autoridad para lograr los objetivos y metas del manejo de seguridad;

b) Los medios y escala de tiempo mediante los cuales las metas y objetivos serán logrados.

Los programas de administración de seguridad serán revisados periódicamente para asegurar que se mantienen efectivos y consistentes con los objetivos y metas. Los programas serán enmendados donde sea necesario.

4.4 Implementación y Operación

4.4.1 Estructura, Autoridad y responsabilidades para la administración de seguridad

La organización establecerá y mantendrá una estructura organizacional de roles, responsabilidades y autoridades, consistente con el logro de su política de manejo de seguridad, objetivos, metas y programas.

Estos roles, responsabilidades y autoridades serán definidos, documentados y comunicados a los individuos responsables por la implementación y mantenimiento.

Los jefes administrativos proveerán evidencia de su compromiso con el desarrollo e implementación de los procesos del sistema de administración de seguridad y mejorar continuamente su efectividad así:

a) Elegir un miembro de administración superior quien, sin tener en cuenta otras responsabilidades, será responsable por el diseño general, mantenimiento, documentación y mejoramiento del sistema de administración de seguridad de la organización.

b) Escoger un miembro de administración con la autoridad necesaria para asegurar que los objetivos y metas sean implementados.

c) Identificando y monitoreando los requerimientos y expectativas de los tenedores de apuestas de la organización y tomar acciones apropiadas y cronometradas para manejar estas expectativas;

d) Asegurar la disponibilidad de recursos adecuados.

e) Considerando el impacto adverso que la política de manejo de seguridad; objetivos, metas, programas, etc. Puedan tener sobre otros aspectos de la organización;

f) Asegurando que otros programas de seguridad generados por otras partes de la organización complementen el sistema de administración de seguridad;

g) Comunicando a la organización la importancia de cumplir con los requerimientos de manejo de seguridad para cumplir con su política;

h) Asegurarse de que las amenazas y riesgos relacionadas con seguridad sean evaluadas e incluidas en las valoraciones de amenazas y riesgos de la organización de forma apropiada;

i) Asegurar la viabilidad de los objetivos, metas y programas de la administración de seguridad.

4.4.2 Competencia, Entrenamiento y Conciencia

La organización se asegurará que el personal responsable por el diseño, operación y manejo de los equipos de seguridad y procesos son cualificados de manera adecuada en términos de educación,

entrenamiento y/ó experiencia. La organización establecerá y mantendrá procedimientos para hacer que las personas que trabajen en el mismo estén conscientes de:

a) La importancia del cumplimiento con la política del manejo de seguridad y procedimientos, y con los requisitos del sistema de la administración de seguridad;
b) Sus roles y responsabilidades en lograr cumplir con la política del manejo de seguridad y procedimientos y con los requisitos del sistema de administración de seguridad, incluyendo preparativos de emergencia y requisitos de respuesta;

c) Las consecuencias potenciales para la seguridad de la organización partiendo de procedimientos operativos específicos.

Se mantendrán registros de competencia y entrenamiento.

4.4.3 Comunicación

La organización tendrá procedimientos para asegurar que la información pertinente del manejo de seguridad sea comunicada a y de los empleados relevantes, contratistas y otros tenedores de apuestas.

Debido a la naturaleza sensible de cierta información relacionada con seguridad, dada la consideración que se debería dar a la sensibilidad de la información antes de la diseminación.

4.4.4 Documentación

La organización establecerá y mantendrá un sistema de documentación de administración de seguridad que incluye, pero no es limitado a lo siguiente:

a) política, objetivos y metas de seguridad,

b) descripción del enfoque del sistema del manejo de seguridad,

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

d) documentos, incluyendo registros requeridos por este estándar internacional, y

e) documentos, incluyendo registros determinados por la organización que sean necesarios para asegurar la planeación efectiva, operación y control de procesos que se relacionan a sus amenazas y riesgos de seguridad.

La organización determinará la sensibilidad de seguridad de la información y tomará pasos para prevenir el acceso no autorizado.

4.4.5 Documento y control de datos

La organización establecerá y mantendrá procedimientos para controlar todos los documentos, datos e información requerida por la cláusula 4 de este estándar internacional para asegurar que:

a) estos documentos, datos e información pueden ser localizados y accesados sólo por individuos autorizados;

b) estos documentos, datos e información son revisados periódicamente, revisados cuando sea necesario, y aprobados por adecuados por personal autorizado;

c) versiones actuales de documentos relevantes, datos e información están disponibles en todas las locaciones donde operaciones esenciales para el funcionamiento efectivo del sistema del manejo de seguridad, se llevan a cabo;

d) documentos obsoletos, datos e información retenidos por propósitos de preservación legal ó de conocimiento son identificados;

e) estos documentos, datos e información son seguros y si son archivados adecuadamente de forma electrónica y pueden ser recuperados.

4.4.6 Control Operativo

La organización identificará aquellas operaciones y actividades que son necesarias para lograr lo siguiente:

a) su política de manejo de seguridad;

b) el control de actividades y mitigación de amenazas identificadas como de alto riesgo;

c) cumplimiento con requisitos de seguridad reguladores y legales;

d) sus objetivos de administración de seguridad;

e) el envío de sus programas de manejo de seguridad;

f) el nivel requerido de la cadena de abastecimiento de seguridad;

La organización se asegurará de que estas operaciones y actividades se lleven a cabo bajo condiciones específicas al:

a) establecer, implementar y mantener procedimientos documentados para controlar situaciones donde su ausencia podría llevar a no lograr las operaciones y actividades listadas en 4.4.6 a) a f);

b) evaluar cualquier amenaza posada desde actividades de la cadena de abastecimiento río arriba y aplicar controles para mitigar estos impactos en la organización y otros operadores de la cadena de abastecimiento río abajo;

c) establecer y mantener los requisitos para bienes y servicios que tengan impacto sobre la seguridad y comunicarlas a proveedores y contratistas;

Estos procedimientos incluirán controles para el diseño, instalación, operación, renovación y modificación de equipos relacionados con seguridad, instrumentación, etc., de manera apropiada. Donde existan arreglos, serán revisados y donde se necesiten serán introducidos, que puedan impactar en las operaciones y actividades del manejo de seguridad, la organización considerará las amenazas y riesgos relacionadas con seguridad antes de su implementación. Los arreglos nuevos ó revisados a ser considerados incluirán lo siguiente:

a) estructura organizacional revisada, roles ó responsabilidades;

b) política, metas, objetivos y programas de manejo de seguridad revisados;

c) procedimientos y procesos revisados;

d) la introducción de nueva infraestructura, equipos de seguridad ó tecnología, que puedan incluir hardware y/ó software;

e) la introducción de nuevos contratistas, proveedores ó personal, como corresponda.

4.4.7 Preparativos de emergencia, respuesta y recuperación de seguridad

La organización establecerá, implementará y mantendrá planes y procedimientos apropiados para identificar el potencial para, y respuestas a, incidentes de seguridad y situaciones de emergencia, y para prevenir y mitigar las consecuencias más probables que puedan estar asociadas con las mismas. Los planes y procedimientos incluirán información de provisión y mantenimiento de todo equipo, servicios e instalaciones identificado que pueda necesitarse durante ó después de situaciones de emergencia ó incidentes.

La organización revisará periódicamente la eficacia de sus preparativos de emergencia, respuesta y planes y procedimientos de recuperación de seguridad, particularmente después de la ocurrencia de incidentes ó situaciones de emergencia causadas por amenazas e incumplimientos de seguridad. La organización evaluará periódicamente estos procedimientos donde apliquen.

4.5 Revisión y acción correctiva

4.5.1 Medida y monitoreo de funcionamiento de seguridad

La organización establecerá y mantendrá procedimientos para monitorear y medir el funcionamiento de su sistema de manejo de seguridad. También establecerá y mantendrá procedimientos para monitorear y medir el funcionamiento de seguridad. La organización considerará las amenazas y riesgos asociadas con seguridad, incluyendo mecanismos de deterioro potencial y sus consecuencias, cuando se establece la frecuencia para medir y monitorear los parámetros de funcionamiento claves, Estos procedimientos proveerán para:

a) tanto medidas cuantitativas como cualitativas, apropiadas para las necesidades de la organización;

b) monitoreando que tanto se cumplen los objetivos, metas y políticas del manejo de seguridad;

c) medidas pro activas de funcionamiento que monitorean el cumplimiento con los programas de manejo de seguridad, criterio de control operativo y legislación aplicable, y otros requisitos reguladores de seguridad;
d) medidas reactivas de funcionamiento para monitorear deterioros, pérdidas, incidentes, inconformismos relacionados con seguridad (incluyendo casi – fallas y falsas alarmas) y otra evidencia histórica de funcionamiento deficiente del sistema de administración de seguridad;

e) Registrando datos y resultados de monitoreo y medición suficiente para facilitar un análisis de acción preventiva y corrección. Si se requiere monitoreo de equipo para el funcionamiento y/ó medición y monitoreo, la organización requerirá el establecimiento y mantenimiento de procedimientos para la calibración y mantenimiento de dicho equipo. Registros de actividades calibración y mantenimiento y sus resultados será retenidos por el tiempo suficiente para cumplir con la legislación y política de la organización.

4.5.2 Evaluación del sistema

La organización evaluará planes, procedimientos y capacidades del manejo de seguridad en revisiones periódicas, tests, reportes después del incidente, lecciones aprendidas, evaluaciones de funcionamiento y ejercicios. Cambios significativos en estos factores deben ser reflejados inmediatamente en el procedimiento.

La organización evaluará el cumplimiento con legislaciones relevantes y regulaciones, mejores prácticas de la industria y conformidad con su propia política y objetivos periódicamente.

La organización mantendrá registros de los resultados de las evaluaciones periódicas.

4.5.3 Fallas, incidentes, inconformidades y acciones correctivas y preventivas relacionadas con seguridad

La organización establecerá, implementará y mantendrá procedimientos para definir responsabilidad y autoridad para:

a) evaluar e iniciar acciones preventivas para identificar fallas potenciales de seguridad y poder evitar que ocurran;

b) la investigación de relacionados con seguridad:

1) fallas incluyendo casi fallas y falsa alarma;

2) incidentes y situaciones de emergencia;

3) inconformidades;

c) tomar acción para mitigar todas las consecuencias dadas de dichas fallas, incidentes ó inconformidades;

d) el inicio y fin de acciones correctivas;

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

Estos procedimientos requerirán que todas las acciones correctivas y preventivas propuestas sean revisadas a través del proceso de valoración de amenaza y riesgo de seguridad antes de la implementación con excepción de que la implementación inmediata anticipe la exposición inminente de la vida ó seguridad pública.

Cualquier acción preventiva ó correctiva tomada para eliminar las causas de inconformidades actuales y potenciales será apropiada para la magnitud de los problemas y proporcional con las posibles amenazas y riesgos del manejo de seguridad. La organización implementará y registrará todos los cambios en los procedimientos documentados que sean el resultado de una acción correctiva y preventiva e incluirá el entrenamiento requerido donde sea necesario.

4.5.4 Control de Registros

La organización establecerá y mantendrá los registros necesarios para demostrar conformidad con los requisitos de su sistema de manejo de seguridad y de este estándar, y de sus logros.

La organización establecerá, implementará y mantendrá procedimientos para la identificación, almacenamiento, protección, retención, recuperación y eliminación de registros.

Habrá registros legibles, identificables y fáciles de encontrar.

Se presentará documentación digital que no se pueda falsificar, con back up seguro y con acceso sólo de personal autorizado.

4.5.5 Auditoria

La organización establecerá, implementará y mantendrá un programa de auditoria de manejo de seguridad y se asegurará que las auditorias del sistema de manejo de seguridad se lleven a cabo en intervalos planeados, para:

a) determinar si el sistema de administración de seguridad:

1) se conforma con arreglos planeados para el manejo de seguridad incluyendo los requisitos de toda la cláusula 4 de esta especificación;

2) ha sido apropiadamente implementada y mantenida;

3) es efectiva en lograr las políticas y objetivos del manejo de seguridad de la organización;

b) revisar los resultados de auditorias previas y las acciones tomadas para rectificar inconformidades;

c) proveer información sobre resultados de auditorias a la administración

d) verificar que el equipo de seguridad y personal sean apropiadamente desplegados.

El programa de auditoria, incluyendo cualquier cronograma, será basado en los resultados de la valoración de amenazas y riesgos de las actividades de la organización y de los resultados de auditorias previas. Los procedimientos de auditorias cubrirán el enfoque, frecuencia, metodologías y competencias, y también las responsabilidades y requisitos para conducir auditorias y reportar resultados. Donde sea posible, las auditorias se llevarán a cabo por personal independiente de aquellos con directa responsabilidad de la actividad que está siendo examinada.

4.6 Revisión administrativa y mejoramiento continuo

La administración superior revisará el sistema de manejo administrativo de la organización, en intervalos planeados, para asegurar que sea apropiado continuamente, adecuación y efectividad. Las revisiones incluirán oportunidades para mejorar y la necesidad de cambios en el sistema de seguridad administrativa, incluyendo política de seguridad y objetivos, amenazas y riesgos de seguridad. Se retendrán los registros de las revisiones administrativas. Aportación a las revisiones administrativas incluirán:

a) resultados de auditorias y evaluaciones de cumplimiento con requisitos legales y con otros requisitos a los que se suscribe la organización;

b) comunicaciones de otras partes interesadas, incluyendo quejas;

c) el funcionamiento de seguridad de la organización;

d) que tanto se ha cumplido con los objetivos y metas,

e) estado de acciones correctivas y preventivas,

f) acciones investigativas de revisiones administrativas anteriores,

g) circunstancias cambiantes, incluyendo desarrollos en requisitos legales y otros relacionados con sus aspectos de seguridad y

h) recomendaciones para mejorar.

Las conclusiones de las revisiones administrativas incluirán todas las decisiones y acciones relacionadas con posibles cambios de la política de seguridad. Objetivos, metas y otros elementos del sistema de manejo administrativo, consistente con el compromiso de mejoramiento continuo.

Anexo A
(informativo)

Correspondencia entre ISO 28000:2007, ISO 14001:2004 y ISO 9001:2000

ISO 28000:2007		ISO 14000:2004		ISO 9001: 2000	
Cadena de abastecimiento De los requisitos del sistema de seguridad administrativa. (Sólo título)	4	Requisitos del sistema de administración ambiental. (Sólo título)	4	Requisitos del sistema De administración de calidad. (sólo título)	4
Requisitos generales	4.1	Requisitos generales	4.1	Requisitos generales	4.1
Política del manejo de Seguridad	4.2	Política ambiental	4.2	Compromiso adminis - trativo 5.1 Política de calidad 5.3 Mejoramiento continuo 8.5.1	
Valoración del riesgo de Seguridad y planeación (sólo título)	4.3	Planeación (sólo título)	4.3	Planeación (sólo título)	5.4
Valoración del riesgo De seguridad	4.3.1	Aspectos ambientales	4.3.1	Enfoque del cliente Determinación de Requisitos relacionados Con el producto 7.2.1 Revisión de requisitos Relacionados con el Producto 7.2.2	5.2
Requisitos legales y Reguladores de seguridad	4.3.2	Requisitos legales y otros	4.3.2	Enfoque del cliente Determinación de Requisitos relacionados	5.2
Objetivos del manejo de Seguridad	4.3.3	Objetivos, metas y progra- Mas	4.3.3	Objetivos de calidad 5.4.1 Planeación del sistema Administrativo de calidad Mejoramiento continuo 8.5.	
Metas del manejo de Seguridad	4.3.4	Objetivos, metas y progra- Mas	4.3.3	Objetivos de calidad 5.4.1 Planeación del sistema Administrativo de calidad Mejoramiento continuo 8.5.	
Programas del manejo De seguridad	4.3.5	Objetivos, metas y progra- Mas	4.3.3	Objetivos de calidad 5.4.1 Planeación del sistema Administrativo de calidad Mejoramiento continuo 8.5.	
Implementación y Operación (sólo título)	4.4	Implementación y operación (sólo título)	4.4	Realización del producto (sólo título)	7

ISO 28000:2007		ISO 14000:2004		ISO 9001: 2000	
Estructura, autoridad y Responsabilidades para El manejo de seguridad	4.4.1	Recursos, roles, responsabilidad y autoridad	4.4.1	Compromiso administrativo Responsabilidad y autoridad Representante administrativo Provisión de recursos Infraestructura	5.1 6.1 6.3
Competencia, entrena-Miento y alerta	4.4.2	Competencia, entrena-Miento y alerta	4.4.2	(Recursos humanos) General Competencia, alerta y Entrenamiento	6.2.1 6.2.2
Comunicación	4.4.3	Comunicación	4.4.3	Comunicación interna Comunicación con Clientes	5.5.3 7.2.3
Documentación	4.4.4	Documentación	4.4.4	(Requisitos de docu-Mentación) general	4.2.1
Documento y control De datos	4.4.5	Control de documentos	4.4.5	Control de documentos	4.2.3
Control operativo	4.4.6	Control operativo	4.4.6	Planeación de Realización de producto	7.1
				Determinación de Requisitos relacionados Con el producto	7.2.1
				Revisión de Requisitos relacionados Con el producto	7.2.2
				Planeación de diseño y Desarrollo	7.3.1
				Aportes de diseño y Desarrollo	7.3.2
				Resultados de diseño y Desarrollo	7.3.3
				Revisión de diseño y Desarrollo	7.3.4
				Verificación del diseño y Desarrollo	7.3.5
				Validación del diseño y Desarrollo	7.3.6
				Control de diseño y Cambios en el desarrollo	7.3.7
				Comprando procesos	7.4.1
				Comprando información	7.4.2
				Verificación del producto Comprado	7.4.3
				Control de producción y Provisión de servicio	7.5.1
				Validación de procesos Para producción y provisión	

				De servicio	7.5.2
ISO 28000:2007		**ISO 14000:2004**		**ISO 9001: 2000**	
				Preservación de producto	7.5.5
Preparación de emergencia, Respuesta y recuperación de Seguridad	4.4.7	Preparación de emergencia Y respuesta	4.4.7	Control de producto Inconforme	8.3
Acción de correctiva y de Chequeo (sólo título)	4.5	Chequeo (sólo título)	4.5	Medición, análisis y Mejoramiento (sólo título)	8
Funcionamiento de seguridad Medición y monitoreo	4.5.1	Monitoreo y medición	4.5.1	Control de monitoreo Y dispositivos de Medición	7.6
				General (medición, Análisis y Mejoramiento)	8.1
				Monitoreo y medición De procesos	8.2.3
				Monitoreo y medición De producto	8.2.4
				Análisis de datos	8.4
Evaluación del sistema	4.5.2	Evaluación de cumplimiento	4.5.2	Monitoreo y medida De procesos	8.2.3
				Monitoreo y medición De producto	8.2.4
Fallas e incidentes Relacionados con seguridad Inconformidades y acciones Preventivas y correctivas	4.5.3	Inconformidad, acción correctiva Y preventiva	4.5.3	Control de producto Inconforme	8.3
				Análisis de datos	8.4
				Acción correctiva	8.5.2
				Acción preventiva	8.5.3
Control de registros	4.5.4	Control de registros	4.5.4	Control de registros	4.2.4
Auditoria	4.5.5	Auditoria interna	4.5.5	Auditoria interna	8.2.2
Revisión administrativa Y mejoramiento continuo	4.6	Revisión administrativa	4.6	Compromiso Administrativo	5.1
				Revisión Administrativa (sólo Título)	5.6
				General	5.6.1
				Aporte de revisión	5.6.2
				Revisión de Producción	5.6.3
				Mejoramiento Continuo	8.5.1

Bibliografía

(1) ISO 9001:2000, Sistemas de administración de seguridad – Requisitos

(2) ISO 14001:2004, Sistemas de administración ambiental – Requisitos con guía para uso

(3) ISO 19011:2002, Guías para calidad y/ó auditoria de sistemas de administración ambiental

(4) ISO/PAS 20858:2004, Tecnología de barcos y marina – Valoraciones de instalaciones de puertos marítimos y desarrollo del plan de seguridad

(5) ISO/PAS 28001, Sistemas de manejo de seguridad para la cadena de abastecimiento – Mejores prácticas para implementar seguridad de la cadena de abastecimiento – Valoraciones y planes

(6) ISO/PAS 28004:2006, Sistemas de administración de seguridad para la cadena de abastecimiento – Guías para la implementación de ISO/PAS 28000