

2008-11-26

**SISTEMAS DE GESTIÓN DE LA SEGURIDAD
PARA LA CADENA DE SUMINISTRO**



E: SPECIFICATION FOR SECURITY MANAGEMENT SYSTEMS
FOR THE SUPPLY CHAIN

CORRESPONDENCIA: esta norma es una adopción idéntica
por traducción (IDT), respecto a su
documento de referencia, la norma
ISO 28000:2007.

DESCRIPTORES: logística; cadena; suministro; sistema
de gestión.

I.C.S.: 47.020.99

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La norma NTC-ISO 28000 fue ratificada por el Consejo Directivo de 2008-11-26.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 172 Transporte terrestre de carga.

ALMACENES GENERALES DE DEPÓSITO	COLSEGUROS
GRAN COLOMBIA S.A. -ALMAGRAN-	ICOLLANTAS
ALPINA S.A.	INLAC
ASOCIACIÓN COLOMBIANA DE	METROPYME
EMPRESAS CARROCERAS -ASCECAR-	QUALITAS INGENIERÍA
AXÓNICA	SERVIENTREGA S.A.
C.I DISAN S.A.	SOANSES. LTDA.
CARROCERÍAS BENFOR	SOCIEDAD TRACTEC
CARROCERÍAS EL SOL	TITADSU
COLFECAR	TRANSPORTE BOTERO SOTO
COLOMBIANA DE TANQUES LTDA.	VALENTINA S.A.
-COLTANQUES LTDA.-	

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

3M COLOMBIA	ALFA SERVICIOS DE GESTIÓN
ABBOTT LABORADORES DE COLOMBIA S.A.	EMPRESARIAL
ACCIÓN SOCIAL - PRESIDENCIA DE LA	ALIMENTOS KRAFT
REPÚBLICA	ALKOSTO
ACERÍAS DE CALDAS S.A.	ALMACENAR
ACERÍAS DE COLOMBIA -ACESCO-	ALMACENES ÉXITO
ACUAVIVA S.A. E.S.P.	ALTHVIZ & CÍA. LTDA.
ACUEDUCTO DE BOGOTÁ	ANALDEX
ALCALDÍA MUNICIPAL DE CALI	ASESORÍAS TÉCNICAS CORREDORES
ALDÍA LOGÍSTICA	DE SEGUROS -ASTEC-

ASOCIACIÓN COLOMBIANA DE LA MICRO,
PEQUEÑAS Y MEDIANAS EMPRESAS -ACOPI-
ASOCIACIÓN COLOMBIANA DEL PESAJE
-ASOPESAJE-
ASOCIACIÓN DE TRANSPORTADORES
INDEPENDIENTES -ATRIN-
ASOCIACIÓN NACIONAL DE INDUSTRIALES
-ANDI-
ASOCIACIÓN NACIONAL DE TRANSPORTADORES
-ASOTRANS-
ASOCIADOS DISTRIBUIDORES DE
DERIVADOS DEL PETRÓLEO -ADISPETROL-
ATENCIÓN TÉCNICA EN CALIDAD LTDA.
AUTO AIRES S..A.
AUTO FUSA S.A.
AVON
BAVARIA S.A.
BEC INTERNATIONAL LTDA.
BUREAU VERITAS CERTIFICATION
C.I. DE AZÚCARES Y MIELES S.A.
C.I. DISAN S.A.
CAFAM
CAJA DE COMPENSACIÓN FAMILIAR
-COMPENSAR-
CAJAS Y SUPLEMENTOS
CÁMARA DE COMERCIO DE CALI
CAMIONES Y REMOLQUES LTDA.
CARULLA
CARVAJAL S.A.
CASA LUKER S.A.
CENTELSA
CENTRALES DE TRANSPORTES S.A.
CENTRORIENTE S.A.
CHALLENGER
CHALLENGER S.A.
CIA COLOMBIANA DE TRANSPORTES S.A.
-COLDETRANS S.A.-
CLÍNICA DE OCCIDENTE S.A.
COCA-COLA - PANAMCO COLOMBIA S.A.
COLCERÁMICA
COLGATE PALMOLIVE
COLOMBIANA KIMBERLY COLPAPEL S.A.
COMFAMA
COMFENALCO SANTANDER
COMPAÑÍA COLOMBIANA AUTOMOTRIZ
COMPAÑÍA DE CARGA MOVITRANSPORTES
LTDA.
COMPAÑÍA DE DISTRIBUCCION Y
TRANSPORTE S.A. -DITRANSA S.A.-
COMPAÑÍA DE GALLETAS NOEL

COMPAÑÍA ESPECIALIZADA EN TRANSPORTES
TERRESTRES LTDA. -CETTA LTDA-
COMPAÑÍA NACIONAL DE CHOCOLATES
COMPAÑÍA NACIONAL DE TRANSPORTE
-CONALTRA-
CONCALIDAD LTDA.
CONCONCRETO S.A.
COOPERATIVA DE TRANSPORTADORES
DEL SUR COTRASUR
COOPERATIVA DE TRANSPORTADORES
VELOTAX LTDA.
COOPERATIVA DE TRANSPORTE DE
CARGA Y LOGÍSTICA
COORDINADORA DE CALIDAD
COORDINADORA INTERNACIONAL DE
CARGA -CORDICARGAS-
CORPORACIÓN ANDINA DE FOMENTO
-CAF-
CORPORACIÓN COLOMBIANA DE LOGÍSTICA
S.A. ALMADELCO - LÓGICA O.T.M.
CORPORACIÓN CYGA
CORPORACIÓN EDUCATIVA MINUTO DE
DIOS
CREDIBANCO VISA
CRITICAL CARGOS ENTER PRICE LTDA.
DESPACHADORA INTERNACIONAL DE
COLOMBIA
DIRECCIÓN DE IMPUESTOS Y ADUANAS
NACIONALES -DIAN-
DUPONT DE COLOMBIA S.A.
ECOPETROL S.A.
EDUARDO BOTERO SOTO Y CÍA LTDA.
EMPRESA COLOMBIANA DE SOPLADO E
INYECCIÓN ECSI S.A.
EMPRESA DE TELECOMUNICACIONES
DE BOGOTÁ -ETB-
ENCLAN S.A.
ENLACE OPERATIVO
EPM BOGOTÁ ESP
ESCUELA COLOMBIANA DE
INGENIERÍA/FACULTAD DE INGENIERÍA
INDUSTRIAL
EXPRESS DEL FUTURO S.A.
EXTRUPLASTIK LTDA.
FABRICATO S.A.
FEDECAME
FEDERACIÓN NACIONAL DE
COMERCIANTES -FENALCO-
FLEXO SPRING S.A.
FORD MOTOR DE COLOMBIA

FORTALEZA DE TRANSPORTES LTDA.
-FORTRANS LTDA.-
G2 CONSULTORES
GASES DEL LLANO S.A. E.S.P. LLANOGAS
GCO SISTEMAS DE GESTIÓN INTEGRAL S.A.
GENERAL MOTORS COLMOTORES
GEOMATRIX S.A.
GESTIÓN DE TECNOLOGÍA LTDA.
GESTIONARTE CONSULTORES
GIMNASIO FEMENINO
GRASCO
GRUPO SIS LTDA.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
IAC
IBM DE COLOMBIA S.A.
INCELT S.A.
INDEPENDIENTE -CARLOS JULIO ROCHA-
INDUSTRIA COLOMBIANA DE LOGÍSTICA Y
TRANSPORTE LTDA. -ICOLTRANS LTDA.-
INDUSTRIA FARMACÉUTICA SYNTOFARMA
S.A.
INDUSTRIA PARA LABORATORIOS S.A.
INDUSTRIAS ALIMENTICIAS NOEL
INDUSTRIAS HACEB S.A.
INDUSTRIAS PHILIPS DE COLOMBIA S.A.
INMOBILIARIA LLERAS E.U.
INTERANDINA DE TRANSPORTE. LTDA.
-INANTRA-
INTERCARGUEROS ANDINOS LTDA.
JOHNSON & JOHNSON DE COLOMBIA S.A.
KENWORTH DE LA MONTAÑA
LABORATORIOS PFIZER S.A.
LAFAYETTE S.A -ZYLETTE S.A.-
LEXCO S.A. CANON
LOGÍSTICA DE TRANSPORTE
LUMINEX S.A.
MARQUES Y URIZA LTDA.
MICHELIN COLOMBIA
MINISTERIO DE COMERCIO, INDUSTRIA Y
TURISMO
MINISTERIO DE TRANSPORTE
MOTORIZADOS EXPRESS LTDA.
MOTOTRANSPORTAR S.A.
MOVISTAR
MULTINACIONAL TRANSPORTADORA LTDA.
MUNDIAL DE ALUMINIOS
MURALLA SEGURIDAD LTDA.
NESTLE DE COLOMBIA
OFIXPRESS
OMNITRACS COLOMBIA
OPEN MARKET
ORGANIZACIÓN TERPEL

PARQUES Y FUNERARIAS S.A.
PETROCOMBUSTIBLES LTDA.
PINTURAS TERINSA
POLICÍA NACIONAL CARRETERAS
PRODUCTOS ALIMENTICIOS DORIA
PROFESIONALES EN DEPORTE
PRODEPORT LTDA. / CGS LTDA.
PROPIETARIOS DE CAMIONES S.A.
-PROCAM S.A.-
PROPILCO S.A.
PROVEEDOR & SERCARGA S.A.
PROVEMEL LTDA.
PROYECTANDO - ASESORÍAS EN GESTIÓN
ORGANIZACIONAL LTDA.
QMS ASESORES
QUINTERO HERMANOS
REDES HUMANAS LTDA.
RETAR INGENIEROS LTDA.
ROJAS TRASTEOS SERVICIO URBANO
BOGOTÁ
SAC
SAMSUNG
SCHRADER CAMARGO S.A.
SECRETARIA DE TRÁNSITO Y
TRANSPORTE
SENA - CENTRO DE GESTIÓN INDUSTRIAL
SIEMENS
SIKA COLOMBIA S.A.
SMS CALIDAD & PROCEDIMIENTOS EU
SOANSES LTDA.
SOLETANCHE BACHY CIMAS S.A.
SSI-SERVICIO DE SALUD INMEDIATO
SUPERINTENDENCIA DE INDUSTRIA Y
COMERCIO
SUPERPOLO S.A.
SURAMERICANA DE TRANSPORTES S.A.
T.D.M. TRANSPORTES S.A.
TANQUES DEL NORDESTE LTDA.
TANQUES Y CAMIONES
TECNICONTROL S.A.
TECNOQUÍMICAS S.A.
TRACTOCARGA LTDA
TRACTOMULAS Y CAMIONES DEL CARIBE
TRÁFICOS Y FLETES S.A.
TRAMAQ
TRANSERVICIOS LTDA.
TRANSGRANOS DE COLOMBIA
TRANSILVHER LTDA.
TRANSPARENCIA POR COLOMBIA
TRANSPORTADORA COMERCIAL COLOMBIANA
-T.C.C.-

TRANSPORTE DE CARGA EXPRESS DE
COLOMBIA LTDA. TRACEXCOL
TRANSPORTES EGO LTDA.
TRANSPORTES ESPECIALIZADOS RTR LTDA.
TRANSPORTES J.R. LTDA.
TRANSPORTES LA PETROLERA VLIMAR
LTDA.
TRANSPORTES M & S S.A.
TRANSPORTES MONRUB & CIA. LTDA.
TRANSPORTES MULTIGRANEL S.A.
TRANSPORTES PREMIER LTDA.
TRANSPORTES SIVAL

TRANSPORTES TERRESTRES DE CARGA
LTDA.
TRANSPORTES VIGIA S.A.
TRANSPORTES VILLAGÓMEZ LTDA.
TRANSPORTES Y SERVICIOS LTDA.
-TRANSER LTDA.-
UNIAGRARIA
UNISYS DE COLOMBIA
UNIVERSIDAD AMÉRICA
UNIVERSIDAD CATÓLICA DE COLOMBIA
UNIVERSIDAD DEL MAGDALENA
YANBAL DE COLOMBIA S.A.

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

	Página
0. INTRODUCCIÓN	1
1. OBJETO Y CAMPO DE APLICACIÓN	2
2. REFERENCIAS NORMATIVAS	3
3. TÉRMINOS Y DEFINICIONES	3
4. ELEMENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD	4
4.1 REQUISITOS GENERALES.....	5
4.2 POLÍTICA DE GESTIÓN DE LA SEGURIDAD.....	5
4.3 EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PLANIFICACIÓN	6
4.4 IMPLEMENTACIÓN Y OPERACIÓN	9
4.5 VERIFICACIÓN Y ACCIÓN CORRECTIVA.....	12
4.6 REVISIÓN POR LA DIRECCIÓN Y MEJORA CONTINUA	14
BIBLIOGRAFÍA.....	19
DOCUMENTO DE REFERENCIA.....	20
FIGURAS	
Figura 1. Relación entre la ISO 28000 y otras normas pertinentes.....	1
Figura 2. Elementos del sistema de gestión de la seguridad.....	4
ANEXOS	
ANEXO A (Informativo)	
CORRESPONDENCIA ENTRE LAS NORMAS ISO 28000:2007, ISO 14001:2004	
E ISO 9001:2000	16

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

0. INTRODUCCIÓN

Esta norma ha sido desarrollada en respuesta a la exigencia de la industria de una norma de gestión de la seguridad. Su objetivo esencial es mejorar la seguridad de las cadenas de suministro. Esta es una norma de gestión de alto nivel que posibilita a una organización establecer un sistema de gestión de la seguridad de la cadena de suministro en general. Exige a la organización evaluar el ambiente de seguridad en el que opera y determinar si se han implementado medidas de seguridad adecuadas y si ya existen otros requisitos de reglamentación que la organización cumple. Si se identifican necesidades de seguridad mediante este proceso, la organización debería implementar mecanismos y procesos para satisfacerlas. Puesto que las cadenas de suministro son dinámicas por naturaleza, algunas organizaciones que manejan múltiples cadenas de suministro pueden buscar que sus proveedores de servicios cumplan las normas ISO de seguridad para la cadena de suministro o las normas gubernamentales relacionadas, como condición para ser incluidos en dicha cadena de suministro a fin de simplificar la gestión de la seguridad, como se ilustra en la Figura 1.

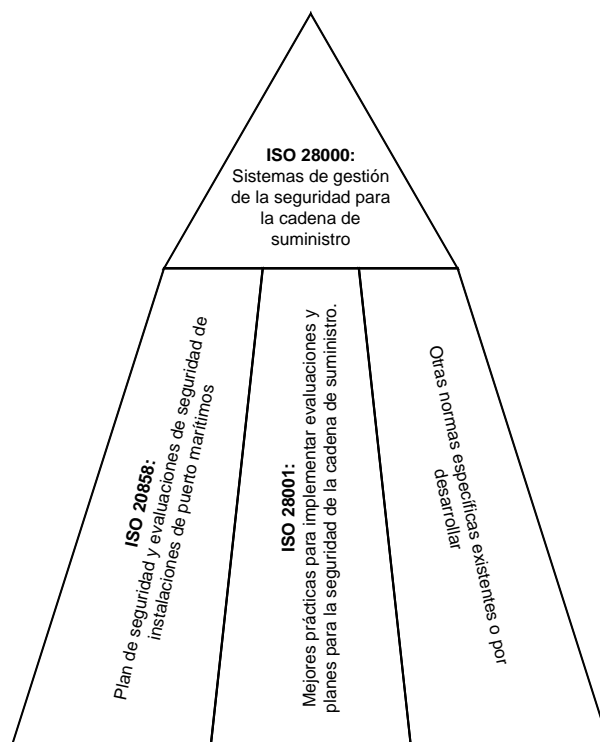


Figura 1. Relación entre la ISO 28000 y otras normas pertinentes

Se prevé la aplicación de la presente norma en casos donde las cadenas de suministro de una organización deben manejarse de manera segura. Un enfoque formal hacia la gestión de la seguridad puede contribuir directamente a la capacidad empresarial y a la credibilidad de la organización.

La conformidad con esta norma no confiere por sí misma exención de las obligaciones legales. Para organizaciones que así lo deseen, pueden verificar la conformidad del sistema de gestión de la seguridad con esta norma mediante un proceso de auditoría externa o interna.

La presente norma se basa en el formato ISO adoptado por la ISO 14001:2004 debido a su enfoque de sistemas de gestión basado en el riesgo. Sin embargo, las organizaciones que han adoptado un enfoque de procesos hacia los sistemas de gestión (por ejemplo ISO 9001:2000) pueden usar su sistema de gestión existente como fundamento para un sistema de gestión de la seguridad, según se prescribe en esta norma. Con esta norma no se pretende duplicar los requisitos y normas gubernamentales concernientes a la gestión de la seguridad de la cadena de suministro con base en las cuales la organización ya se ha certificado o se ha verificado su conformidad. La verificación puede realizarla una organización aceptable por primera, segunda o tercera parte.

NOTA Esta norma se basa en la metodología conocida como Planificar-Hacer-Verificar-Actuar (PHVA). PHVA se puede describir de la siguiente manera:

- Planificar: Establecer los objetivos y procesos necesarios para entregar resultados de acuerdo con la política de seguridad de la organización.
- Hacer: Implementar los procesos.
- Verificar: Supervisar y medir procesos contra la política de seguridad, objetivos, metas, requisitos legales y otros y reportar resultados.
- Actuar: Tomar acciones para mejorar continuamente el desempeño del sistema de gestión de la seguridad.

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma especifica los requisitos para un sistema de gestión de la seguridad, incluidos 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 empresarial, que incluyen todas las actividades controladas o influenciadas por organizaciones que impacta en la seguridad de la cadena de suministro. Estos otros aspectos se deberían considerar directamente cuando y donde tengan impacto en la gestión de la seguridad, incluido el transporte de estos bienes a lo largo de la cadena de suministro.

La presente norma es aplicable a organizaciones de todos los tamaños, desde las pequeñas hasta las multinacionales, de manufactura, servicios, almacenamiento o transporte en cualquier etapa de la producción o la cadena de suministro que desee:

- 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 ante otros;
- d) buscar certificación/registro de su sistema de gestión de la seguridad por un organismo de certificación de tercera parte, acreditado; o

- e) realizar una auto-determinación y auto-declaración de la conformidad con esta norma.

Existen códigos legislativos y de reglamentación que abordan algunos de los requisitos de esta norma.

Esta norma no pretende exigir una doble demostración de la conformidad.

Las organizaciones que optan por la certificación por una tercera parte pueden demostrar además que están contribuyendo significativamente a la seguridad de la cadena de suministro.

2. REFERENCIAS NORMATIVAS

No se citan normas de referencia. Se incluye este numeral para conservar el esquema de numerales similar a otras normas de sistemas de gestión.

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de esta norma se aplican los términos y definiciones siguientes:

3.1 Instalación. Planta, maquinaria, propiedad, edificios, vehículos, embarcaciones, instalaciones portuarias y otros elementos de infraestructura o plantas y sistemas relacionados que cumplen una función o servicio empresarial distintivo y cuantificable.

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

3.2 Seguridad. Resistencia a actos intencionales, sin autorización, destinados a causar perjuicio o daño a, o mediante, la cadena de suministro.

3.3 Gestión de la seguridad. Actividades y prácticas sistemáticas y coordinadas por medio de las cuales una organización maneja óptimamente sus riesgos y las amenazas e impactos potenciales asociados derivados de ellos.

3.4 Objetivo de gestión de la seguridad. Resultado o logro específico de seguridad requerido a fin de cumplir la política de gestión de la seguridad.

NOTA Es esencial que dichos resultados se relacionen directa o indirectamente con la entrega de productos, suministros o servicios prestados por la totalidad de la empresa a sus clientes o usuarios finales.

3.5 Política de gestión de la seguridad. Intenciones y direcciones generales de una organización, relacionadas con la seguridad y la estructura para el control de los procesos y actividades que tienen que ver con la seguridad, que se derivan de la política y los requisitos de reglamentación de la organización y son coherentes con ellos.

3.6 Programas de gestión de la seguridad. Medios por los cuales se logra un objetivo de gestión de la seguridad.

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

3.8 Parte involucrada. Persona o entidad con un interés establecido en el desempeño de la organización, su éxito o el impacto de sus actividades.

NOTA Son ejemplos: los clientes, accionistas, entidades financieras, aseguradoras, reglamentadores, organismos estatutarios, empleados, contratistas, proveedores, agremiaciones laborales, o la sociedad.

3.9 Cadena de suministro. Conjunto relacionado de recursos y procesos que comienza con el suministro de materias primas y se extiende hasta la entrega de productos o servicios al usuario final, incluidos los medios de transporte.

NOTA La cadena de suministro puede incluir vendedores, instalaciones de manufactura, proveedores de logística, centros de distribución interna, distribuidores, 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 sale del control operacional directo de la organización, incluidas la gestión de los seguros, las finanzas y los datos, y el empaque, almacenamiento y transferencia de la carga, entre otros.

3.9.2 Aguas arriba. Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro, que ocurren antes de que la carga se encuentre bajo el control operacional de la organización, incluida la gestión de datos, las finanzas y los seguros y el empaque, almacenamiento y transferencia de la carga, entre otros.

3.10 Alta dirección. Persona o grupo de personas que dirige y controla una organización en el nivel superior.

NOTA Es posible que la alta dirección, especialmente en una gran organización multinacional, no esté involucrada personalmente como se describe en la presente norma; sin embargo, la responsabilidad de la alta dirección a través de la cadena de mando debe ser manifiesta.

3.11 Mejora continua. Proceso recurrente de fortalecer el sistema de gestión de la seguridad a fin de lograr mejoras en el desempeño de la seguridad en general de manera 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 establecer, documentar, implementar, mantener y mejorar continuamente 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 continuamente su eficacia de acuerdo con los requisitos establecidos en todo el numeral 4.

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

4.2 POLÍTICA DE GESTIÓN DE LA SEGURIDAD

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

- a) ser coherente con otras políticas organizacionales;
- b) proporcionar el marco de referencia para establecer objetivos, metas y programas específicos de gestión de la seguridad;
- c) ser coherente con la estructura de la gestión de amenazas y riesgos de la seguridad general de la organización;
- d) ser apropiada para las amenazas de la organización y la naturaleza y escala de sus operaciones;
- e) determinar claramente los objetivos generales/amplios de gestión de la seguridad;
- f) incluir un compromiso con la mejora continua del proceso de gestión de la seguridad;
- g) incluir un compromiso de cumplir con la legislación actual aplicable, los requisitos de reglamentación y estatutarios y otros requisitos que suscribe la organización;
- h) tener el respaldo visible de la alta dirección;
- i) ser documentada, implementada y mantenida;
- j) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas y visitantes, con la intención de que estas personas sean conscientes de sus obligaciones individuales relacionadas con la gestión de la seguridad;
- k) estar disponible para las partes interesadas, cuando resulte apropiado;
- l) poderse revisar en caso de adquisición o fusión con otras organizaciones, u otro cambio en el alcance del negocio de la organización que pueda afectar la continuidad o pertinencia del sistema de gestión de la seguridad.

NOTA Las organizaciones pueden optar por una política de gestión de la seguridad detallada para uso interno que ofrezca suficiente información y dirección para orientar el sistema de gestión de la seguridad (algunas partes de éste pueden ser confidenciales) y una versión resumida (no confidencial) que contenga los objetivos generales para divulgación entre sus partes involucradas y otras partes interesadas.

4.3 EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PLANIFICACIÓN

4.3.1 Evaluación del riesgo de seguridad

La organización debe establecer y mantener procedimientos para la identificación y evaluación continua de las amenazas a la seguridad y de las amenazas y riesgos relacionados con la gestión de la seguridad y la identificación e implementación de medidas necesarias de control de gestión. La identificación, evaluación y los métodos de control de amenazas y riesgos de la seguridad 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, que deben incluir:

- a) amenazas y riesgos de falla física, tales como falla funcional, daño incidental, daño malicioso o terrorista o acción criminal;
- b) amenazas y riesgos operacionales, incluidos el control de la seguridad, los factores humanos y otras actividades que afectan el desempeño, la condición o la seguridad de las organizaciones;
- c) eventos del medio ambiente natural (tormentas, inundaciones, etc.) que pueden hacer que las medidas y equipos de seguridad resulten ineficaces;
- d) factores por fuera del control de la organización, tales como fallas en el equipo y servicios suministrados externamente;
- e) amenazas y riesgos de las partes involucradas, tales como falla en cumplir los requisitos de reglamentación o daño a la reputación o la marca;
- f) diseño e instalación del equipo de seguridad, incluido su reemplazo, mantenimiento, etc.;
- g) gestión de datos e información y comunicaciones;
- h) una amenaza a la continuidad de las operaciones.

La organización debe asegurar que se consideren los resultados de estas evaluaciones y los efectos de estos controles y, cuando resulte apropiado, debe proporcionar elementos de entrada a:

- a) los objetivos y metas de gestión de la seguridad;
- b) los programas de gestión de la seguridad;
- c) la determinación de requisitos para el diseño, especificación e instalación;
- d) la identificación de recursos adecuados, incluidos los niveles de contratación de personal;
- e) la identificación de necesidades de formación y habilidades (véase el numeral 4.4.2);
- f) el desarrollo de controles operacionales (véase el numeral 4.4.6);

g) la estructura general de gestión de amenazas y riesgos de la organización.

La organización debe documentar y mantener actualizada la anterior información.

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

- a) estar definida con respecto a su alcance, naturaleza y programación en el tiempo, para asegurar que sea proactiva en vez de reactiva;
- b) incluir la información recolectada acerca de las amenazas y riesgos de la seguridad;
- c) proporcionar la clasificación de amenazas y riesgos y la identificación de aquellos que deben evitarse, eliminarse o controlarse;
- d) proporcionar el seguimiento de las acciones para garantizar su eficacia y oportuna implementación (véase el numeral 4.5.1).

4.3.2 Requisitos de seguridad legales, estatutarios y otros regulatorios

La organización debe establecer, implementar y mantener un procedimiento:

- a) para identificar y tener acceso a los requisitos legales aplicables y otros requisitos que suscribe la organización en relación con sus amenazas y riesgos para la seguridad, y
- b) para determinar cómo se aplican estos requisitos a sus amenazas y riesgos para la seguridad.

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

4.3.3 Objetivos de gestión de la seguridad

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

- a) requisitos legales, estatutarios y otros de reglamentación sobre seguridad;
- b) amenazas y riesgos relacionados con la seguridad;
- c) opciones tecnológicas y otras;
- d) requisitos financieros, operacionales y empresariales;
- e) puntos de vista de las partes interesadas apropiadas.

Los objetivos de gestión de la seguridad deben:

- a) ser coherentes con el compromiso de la organización con la mejora continua;
- b) cuantificarse (cuando sea posible);

- c) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas, con la intención de que tales personas sean conscientes de sus obligaciones individuales;
- d) revisarse periódicamente para garantizar que sigan siendo pertinentes y coherentes con la política de gestión de la seguridad. Cuando sea necesario, se deben corregir de acuerdo con los objetivos de gestión de la seguridad.

4.3.4 Metas de gestión de la seguridad

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

Estas metas deben:

- a) tener un nivel apropiado de detalles;
- b) ser específicos, medibles, obtenibles, pertinentes y con base en el tiempo (cuando sea aplicable);
- c) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas, con la intención de que tales personas sean conscientes de sus obligaciones individuales;
- d) revisarse periódicamente para asegurar que sigan siendo pertinentes y coherentes con los objetivos de gestión de la seguridad. Donde sea necesario las metas se deben ajustar consecuentemente.

4.3.5 Programas de gestión de la seguridad

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

Los programas deben optimizarse y luego priorizarse y la organización debe prever el uso de los costos de manera eficiente y eficaz en la implementación de estos programas.

Se debe incluir documentación que describa:

- a) la responsabilidad y autoridad designada para lograr objetivos y metas de gestión de la seguridad;
- b) los medios y la escala en el tiempo por medio de los cuales se logran los objetivos y metas de gestión de la seguridad.

Los programas de gestión de la seguridad deben revisarse periódicamente para asegurar que se mantienen efectivos y coherentes con los objetivos y metas. Cuando sea necesario, los programas se deben ajustar consecuentemente.

4.4 IMPLEMENTACIÓN Y OPERACIÓN

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

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

Estas funciones, responsabilidades y autoridades se deben definir, documentar y comunicar a los individuos responsables de la implementación y mantenimiento.

La alta dirección debe presentar evidencia de su compromiso con el desarrollo e implementación del sistema de gestión de la seguridad (procesos) y mejorar continuamente su eficacia mediante las siguientes acciones:

- a) nombrar un miembro de la alta dirección quien, independientemente de sus otras responsabilidades, debe ser responsable del diseño, mantenimiento, documentación y mejora generales del sistema de gestión de la seguridad de la organización;
- b) nombrar un miembro (o varios) de la dirección, con la autoridad necesaria para garantizar que se implementen los objetivos y metas;
- c) identificar y hacer seguimiento a los requisitos y expectativas de las partes interesadas de la organización y emprender las acciones apropiadas y oportunas para manejar dichas expectativas;
- d) garantizar la disponibilidad de recursos adecuados;
- e) considerar el impacto adverso que la política, los objetivos, las metas, los programas, etc., de gestión de la seguridad pueden tener en otros aspectos de la organización;
- f) garantizar que cualquier programa de seguridad generado por otras partes de la organización complemente el sistema de gestión de la seguridad;
- g) comunicar a la organización la importancia de cumplir sus requisitos de gestión de la seguridad a fin de cumplir con su política;
- h) garantizar que las amenazas y riesgos relacionados con la seguridad sean evaluados y se incluyan en evaluaciones de amenazas y riesgos organizacionales, según resulte apropiado;
- i) garantizar la viabilidad de los objetivos, metas y programas de gestión de la seguridad.

4.4.2 Competencia, entrenamiento y toma de conciencia

La organización debe garantizar que el personal responsable del diseño, operación y gestión de equipos y procesos de seguridad esté calificado adecuadamente en lo relativo a educación, entrenamiento o experiencia o ambas. La organización debe establecer y mantener procedimientos para que las personas que trabajan para ella o en su nombre sean conscientes de:

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

- b) sus funciones y responsabilidades en el logro de la conformidad con la política y procedimientos de gestión de la seguridad y con los requisitos del sistema de gestión de la seguridad, incluidos los requisitos de preparación y respuesta ante emergencias;
- c) las consecuencias potenciales que tiene para la seguridad de la organización desviarse de los procedimientos de operación especificados.

Se deben llevar registros de competencia y entrenamiento.

4.4.3 Comunicación

La organización debe contar con procedimientos para asegurar que la información pertinente de gestión de la seguridad se comunica hacia y desde los empleados relevantes, contratistas y otras partes interesadas.

Debido a la naturaleza confidencial de alguna información relacionada con la seguridad, se debería considerar adecuadamente la sensibilidad de la información antes de su divulgación.

4.4.4 Documentación

La organización debe establecer y mantener un sistema de documentación de gestión de la seguridad que incluya los siguientes aspectos (sin limitarse a ellos):

- a) la política, objetivos y metas de 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 referencia con documentos relacionados:
- d) los documentos, incluidos registros, exigidos en la presente norma, y
- e) los documentos, incluidos los registros, determinados por la organización como necesarios para garantizar la planificación, operación y control eficaces de los procesos relacionados con sus amenazas y riesgos para la seguridad significativos.

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

4.4.5 Control de documentos y datos

La organización debe establecer y mantener procedimientos para controlar todos los documentos, datos e información exigidos en el numeral 4 de la presente norma a fin de garantizar que:

- a) sólo individuos autorizados puedan localizar y tener acceso a estos documentos, datos e información;
- b) personal autorizado revise periódicamente estos documentos, datos e información, los actualice según sea necesario y apruebe su conveniencia;
- c) se encuentren disponibles versiones actuales de los documentos, datos e información pertinentes en todos los lugares donde se realicen operaciones esenciales para el funcionamiento efectivo del sistema de gestión de la seguridad;

- d) los documentos, datos e información obsoletos sean retirados con prontitud de todos los puntos de emisión y de uso, o se asegure de otro modo que no se haga uso indeseado de ellos;
- e) se identifiquen adecuadamente los documentos de archivo, datos e información que se conservan con propósitos legales o de preservación del conocimiento, o ambos;
- f) dichos documentos, datos e información sean seguros y si se encuentran en formato electrónico, deben tener copia de seguridad adecuada y se puedan recuperar.

4.4.6 Control operacional

La organización debe identificar aquellas operaciones y actividades que sean necesarias para lograr:

- a) su política de gestión de la seguridad;
- b) el control de las actividades y la mitigación de amenazas identificadas como un riesgo significativo;
- c) la conformidad con requisitos legales, estatutarios y otros requisitos de reglamentación sobre seguridad;
- d) sus objetivos de gestión de la seguridad;
- e) la ejecución de sus programas de gestión de la seguridad;
- f) el nivel requerido de seguridad de la cadena de suministro.

La organización debe garantizar que estas operaciones y actividades se realicen bajo las condiciones especificadas mediante:

- a) el establecimiento, implementación y mantenimiento de procedimientos documentados para controlar situaciones en las que su ausencia podría conducir a falla en el logro de las operaciones y actividades enunciadas en el numeral 4.4.6, literales a) a f);
- b) la evaluación de cualquier amenaza que surja de las actividades aguas arriba de la cadena de suministro, y aplicación de controles para mitigar estos impactos en la organización y otros operadores aguas abajo de la cadena de suministro;
- c) el establecimiento y mantenimiento de los requisitos para bienes y servicios que tienen impacto en la seguridad, y comunicación de estos a proveedores y contratistas.

Estos procedimientos deben incluir controles para el diseño, instalación, operación, renovación y modificación de elementos de equipos, instrumentación etc., relacionados con la seguridad, según resulte apropiado. Cuando se actualicen las disposiciones existentes o se introduzcan nuevas que puedan causar impacto en las operaciones y actividades de gestión de la seguridad, la organización debe considerar las amenazas y riesgos de la seguridad asociados antes de su implementación. Las disposiciones nuevas o actualizadas que se vayan a considerar deben incluir:

- a) la estructura, funciones o responsabilidades organizacionales actualizadas;
- b) la política, objetivos, metas o programas de gestión de la seguridad actualizados;

- c) los procesos y procedimientos actualizados;
- d) la introducción de nueva infraestructura, equipos o tecnología de seguridad que pueden incluir hardware o software, o ambos;
- e) la introducción de nuevos contratistas, proveedores o personal, según sea apropiado.

4.4.7 Preparación y respuesta ante emergencias y recuperación de la seguridad

La organización debe establecer, implementar y mantener planes y procedimientos apropiados para identificar el potencial y las respuestas ante incidentes de seguridad y situaciones de emergencia, y para evitar y mitigar las consecuencias probables que se puedan asociar con ellos. Los planes y procedimientos deben incluir información acerca de la disposición y mantenimiento de cualquier equipo, instalaciones o servicios identificados que puedan requerirse durante o después de los incidentes o situaciones de emergencia.

La organización debe revisar periódicamente la eficacia de sus planes y procedimientos de preparación y respuesta ante emergencias y recuperación de la seguridad, en especial después de que ocurren incidentes o situaciones de emergencia causados por infracciones y amenazas a la seguridad. La organización debe poner a prueba periódicamente estos procedimientos, cuando sea aplicable.

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 seguimiento y medir el desempeño de su sistema de gestión de la seguridad. Además, debe establecer y mantener procedimientos para el seguimiento y medición del desempeño de la seguridad. Al establecer la frecuencia de medición y seguimiento de los parámetros de desempeño clave, la organización debe considerar las amenazas y riesgos de seguridad asociados, incluidos los mecanismos de deterioro potencial y sus consecuencias. Estos procedimientos deben proporcionar:

- a) medidas tanto cualitativas como cuantitativas, apropiadas para las necesidades de la organización;
- b) seguimiento del grado en el que se cumplen la política, objetivos y metas de la gestión de la seguridad de la organización;
- c) medidas proactivas de desempeño para hacer el seguimiento a la conformidad con los programas de gestión de la seguridad, los criterios de control operacionales y la legislación aplicable, los requisitos estatutarios y otros requisitos de reglamentación sobre seguridad;
- d) medidas reactivas de desempeño para hacer el seguimiento de deterioro, fallas, incidentes, no conformidades (incluidas las fallas que estuvieron a punto de ocurrir y las falsas alarmas) relacionadas con la seguridad y otra evidencia histórica de desempeño deficiente del sistema de gestión de la seguridad;
- e) registro de datos y resultados de seguimiento y medición suficientes para facilitar el análisis de las acciones preventivas y correctivas posteriores. Si se requiere equipo de seguimiento para el desempeño, y la medición o seguimiento, o todos ellos, la organización debe exigir que se establezcan y mantengan procedimientos para la calibración y mantenimiento de dicho equipo. Se deben conservar registros de las

actividades de calibración y mantenimiento durante tiempo suficiente, para cumplir con la legislación y la política de la organización.

4.5.2 Evaluación del sistema

La organización debe evaluar los planes, procedimientos y capacidades de gestión de la seguridad por medio de revisiones periódicas, ensayos, informes posteriores a los incidentes, lecciones aprendidas, evaluaciones de desempeño y ejercicios. Los cambios significativos en estos factores deben reflejarse de inmediato en el (los) procedimiento(s).

La organización debe evaluar periódicamente la conformidad con la legislación y las reglamentaciones pertinentes, las mejores prácticas industriales y la conformidad con su propia política y objetivos.

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

4.5.3 Fallas relacionadas con la seguridad, incidentes, no conformidades y acciones correctivas y preventivas

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

- a) evaluar e iniciar acciones preventivas para identificar las fallas potenciales en la seguridad, a fin de que se pueda evitar que ocurran;
- b) investigar los siguientes aspectos relacionados con la seguridad:
 - 1) fallas, incluidas las que estuvieron a punto de ocurrir, y las falsas alarmas;
 - 2) incidentes y situaciones de emergencia;
 - 3) no conformidades;
- c) emprender acciones para mitigar cualquier consecuencia de dichas fallas, incidentes o no conformidades;
- d) iniciar y completar las acciones correctivas;
- e) confirmar la eficacia de las acciones correctivas emprendidas.

Estos procedimientos deben exigir que se revisen todas las acciones correctivas y preventivas propuestas por medio del proceso de evaluación de amenazas y riesgos de seguridad antes de la implementación, a menos que la implementación inmediata impida exposiciones inminentes para la vida o seguridad pública.

Cualquier acción correctiva o preventiva emprendida para eliminar las causas de no conformidades reales y potenciales debe ser apropiada para la magnitud de los problemas y proporcional a las amenazas y riesgos de la seguridad que probablemente se encuentren. La organización debe implementar y registrar cualquier cambio en los procedimientos documentados que resulten de la acción correctiva y preventiva y debe incluir el entrenamiento requerida cuando fuera necesario.

4.5.4 Control de registros

La organización debe establecer y mantener registros, según sea necesario, para demostrar conformidad con los requisitos de su sistema de gestión de la seguridad y de esta norma, y de los resultados logrados.

La organización debe establecer, implementar y mantener un procedimiento (o varios) para la identificación, almacenamiento, protección, recuperación, retención y disposición de registros.

Los registros deben ser legibles y permanecer así, y deben ser identificables y trazables.

La documentación electrónica y digital debería estar protegida contra alteración, tener copia de seguridad y ser accesible sólo a personal autorizado.

4.5.5 Auditoría

La organización debe establecer, implementar y mantener un programa de auditoría de gestión de la seguridad y debe garantizar que las auditorías del sistema de gestión de la seguridad se realicen a intervalos planificados, a fin de:

- a) determinar si el sistema de gestión de la seguridad:
 - 1) cumple las disposiciones planificadas para gestión de la seguridad, incluidos los requisitos de la totalidad del numeral 4 de la presente norma;
 - 2) ha sido implementado y se mantiene adecuadamente;
 - 3) es eficaz para cumplir la política y objetivos de gestión de la seguridad de la organización;
- b) revisar los resultados de auditorías anteriores y las acciones emprendidas para rectificar las no-conformidades;
- c) proporcionar información a la dirección sobre los resultados de las auditorías;
- d) verificar el despliegue apropiado de los equipos y del personal de seguridad.

El programa de auditoría, incluido cualquier cronograma, debe estar basado en los resultados de las evaluaciones de amenazas y riesgos de las actividades de la organización y en los resultados de auditorías anteriores. Los procedimientos de auditoría deberían comprender el alcance, la frecuencia, las metodologías y competencias, lo mismo que las responsabilidades y requisitos para realizar auditorías y reportar resultados. Cuando sea posible, las auditorías las debe llevar a cabo personal independiente de los que tienen responsabilidad directa en la actividad que se está examinando.

NOTA La frase "personal independiente" no necesariamente significa 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, a fin de garantizar que siga siendo conveniente, suficiente y eficaz. Las revisiones deben incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el sistema de gestión de la seguridad, incluida la política de seguridad, los objetivos, y las amenazas y los riesgos de la seguridad. Se deben retener registros de las revisiones realizadas por la dirección. La información de entrada de las revisiones por la dirección debe incluir:

- a) resultados de las auditorías y evaluaciones de conformidad con los requisitos legales y con otros requisitos que suscribe la organización;
- b) comunicación (es) de partes externas interesadas, incluidas quejas;
- c) el desempeño de la seguridad de la organización;
- d) el grado en el que se cumplen objetivos y metas;
- e) estado de las acciones correctivas y preventivas;
- f) acciones de seguimiento de revisiones por la dirección anteriores;
- g) circunstancias cambiantes, incluidos desarrollos en requisitos legales y otros, relacionados con aspectos de su seguridad, y
- h) recomendaciones de mejora.

La información de salida de las revisiones por la dirección debe incluir cualquier decisión y acción relacionada con cambios posibles a la política, objetivos, metas y otros elementos del sistema de gestión de la seguridad, de manera coherente con el compromiso con la mejora continua.

ANEXO A
(Informativo)

**CORRESPONDENCIA ENTRE LAS NORMAS ISO 28000:2007,
ISO 14001:2004 E 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 (sólo título)	4	Requisitos del sistema de gestión ambiental (sólo título)	4	Requisitos del sistema de gestión de la calidad (sólo título)	4
Requisitos generales	4.1	Requisitos generales	4.1	Requisitos generales	4.1
Política de gestión de la seguridad	4.2	Política ambiental	4.2	Compromiso de la dirección	5.1
				Política de la calidad	5.3
				Mejora continua	8.5.1
Evaluación del riesgo de seguridad y planificación (sólo título)	4.3	Planificación (sólo título)	4.3	Planificación (sólo título)	5.4
Evaluación del riesgo de seguridad	4.3.1	Aspectos ambientales	4.3.1	Enfoque al cliente	5.2
				Determinación de los requisitos relacionados con el producto	7.2.1
				Revisión de los requisitos relacionados con el producto	7.2.2
Requisitos legales, estatutarios y otros requisitos reglamentarios sobre seguridad	4.3.2	Requisitos legales y otros	4.3.2	Enfoque al cliente	5.2
				Determinación de los requisitos relacionados con el producto	7.2.1
Objetivos de gestión de la seguridad	4.3.3	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Objetivos de gestión de la seguridad	4.3.4	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Programa(s) de gestión de la seguridad	4.3.5	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Implementación y operación (sólo título)	4.4	Implementación y operación (sólo título)	4.4	Realización del producto (sólo título)	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	5.1
				Responsabilidad y autoridad	5.5.1
				Representante de la dirección	5.5.2
				Provisión de recursos	6.1
				Infraestructura	6.3

Continúa...

(Continuación)

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Competencia, entrenamiento y toma de conciencia	4.4.2	Competencia, entrenamiento y toma de conciencia	4.4.2	(Recursos humanos) Generalidades	6.2.1
				Competencia, entrenamiento y toma de conciencia	6.2.2
Comunicación	4.4.3	Comunicación	4.4.3	Comunicación interna	5.5.3
				Comunicación con el cliente	7.2.3
Documentación	4.4.4	Documentación	4.4.4	(Requisitos de la documentación) Generalidades	4.2.1
Control de documentos y datos	4.4.5	Control de documentos	4.4.5	Control de 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 cambios del diseño y desarrollo	7.3.7
				Proceso de compras	7.4.1
				Información de las compras	7.4.2
				Verificación de los productos comprados	7.4.3
				Control de la producción y de la prestación del servicio	7.5.1
Validación de los procesos de producción y de prestación del servicio	7.5.2				
Preservación del producto	7.5.5				
Preparación y respuesta ante emergencias y recuperación de la seguridad	4.4.7	Preparación y respuesta ante emergencias	4.4.7	Control del producto no conforme	8.3

NORMA TÉCNICA COLOMBIANA NTC-ISO 28000

(Final)

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Verificación y acción correctiva (sólo título)	4.5	Verificación (sólo título)	4.5	Medición, análisis y mejora (sólo título)	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 de conformidad	4.5.2	Seguimiento y medición de los procesos	8.2.3
				Seguimiento y medición del producto	8.2.4
Fallas relacionadas con la seguridad, incidentes, no conformidades y acciones correctivas y preventivas	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 registros	4.5.4	Control de 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 (sólo título)	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 auditoria de los sistemas de gestión de la calidad y/o ambiente.
- [4] ISO/PAS 20858:2004, *Ships and Marine Technology. Maritime Port Facility Security Assessments and Security Plan Development.*
- [5] ISO/PAS 28001, *Security Management Systems for the Supply Chain. Best Practices for Implementing Supply Chain Security. Assessments and Plans.*
- [6] ISO/PAS 28004:2006, *Security Management Systems for the Supply Chain. Guidelines for the Implementation of ISO/PAS 28000.*

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Specification for Security Management Systems for the Supply Chain*. Geneva, Switzerland, ISO: 28000: 2007(E), p 16.