COMPENDIO

ICONTEC

ISO 28000

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

CONTENIDO

INTRODUCCIÓN

ICONTEC, en su calidad de organismo nacional de normalización, según el Decreto 2269 de 1993, desarrolla los documentos normativos que unifican los criterios a través del consenso, dentro del trabajo de sus comités técnicos,

Esos documentos normativos, entre los que se incluyen las Normas Técnicas Colombianas (NTC), son de aplicación voluntaria y permiten a los sectores productivos y de servicios competir en los mercados internacionales. Por esta razón, la elaboración de estos documentos también atiende las recomendaciones de la Organización Mundial del Comercio (OMC), la cual define que los reglamentos técnicos elaborados por el Gobierno Nacional deben basarse en normas técnicas internacionales o nacionales.

Con este propósito, los comités técnicos relacionados con sistemas de gestión y el 172 de Transporte Terrestre de carga conformaron un grupo interdisciplinario de profesionales representantes de la industria, los consumidores, el gobierno y los intereses generales, el cual estableció un conjunto de requisitos fundamentales de calidad, seguridad, protección a la salud y el medio ambiente, para la normalización relacionada con el transporte de mercancías en general y la gestión, incluyendo sistemas de calidad. Como resultado de esta labor, se publica la serie de normas NTC-ISO 28000 que incluye:

- NTC-ISO 28000, Sistemas de gestión de la seguridad para la cadena de suministro;
- NTC-ISO 28001, Sistemas de gestión de la seguridad para la cadena de suministro. Mejores prácticas para implementar evaluaciones y planes para la seguridad de la cadena de suministro. Requisitos y orientación, y la
- NTC-ISO 28004, Sistemas de gestión de la seguridad para la cadena de suministro. Directrices para la implementación de la norma ISO 28000.

Estas normas se basan en los documentos de referencia ISO 28000 de la Organización Internacional de Normalización (ISO), lo cual asegura la unificación de criterios y la transferencia tecnológica, fundamentales para facilitar el comercio, la cooperación tecnológica y comprensión mutua entre las partes.

En efecto, la serie de normas NTC-ISO 28000 define requisitos y recomendaciones para organizaciones de cualquier tamaño y tipo que estén involucradas en las cadenas de suministros, entendiéndose como cadena de suministros el conjunto relacionado de recursos y procesos que comienza con el suministro de materias primas hasta la entrega del producto o servicio al usuario final, a través de los diferentes modelos de transporte (marítimo, terrestre o aéreo). Su propósito es suministrar productos garantizados y seguros para el usuario final.

Los incidentes de seguridad contra las cadenas de suministros son amenazas latentes para todo tipo de organización, las cuales han tomado conciencia de la necesidad de protección sobre sus bienes, personal, infraestructura y equipos. Por esto mismo, el

uso de un sistema de gestión para la seguridad para la cadena de suministro combina las diferentes necesidades de estas organizaciones con una serie de requisitos y análisis, para conocer los puntos de control y actuar contra los posibles riesgos y amenazas, con base en la evaluación y la planificación de los riesgos que afectan a la organización y el establecimiento de medidas y técnicas que garanticen la seguridad del servicio. En el análisis de riesgos, la organización debe valorar todas aquellas amenazas existentes para su organización, su impacto en caso de materializarse e implementar aquellas medidas de prevención y mitigación.

Esta serie es compatible con las normas de sistemas de gestión NTC-ISO 9001 y NTC-ISO 14001, lo cual facilita la integración de los sistemas de gestión de la cadena de suministro, de calidad y ambiental de las organizaciones. En razón a que la NTC-ISO 28000 es una de las familias de normas basadas en los sistemas de gestión, tiene como fundamento la metodología planificar - hacer - verificar - actuar (PHVA), la cual hace que las organizaciones sean capaces de:

- Planificar, implementar, usar, mantener y actualizar un sistema de gestión para la seguridad de la cadena de suministros cuyo propósito consiste en suministrar productos o servicios o ambos, que sean seguros para el usuario.
- Examinar y evaluar los requisitos del cliente y los acuerdos que los clientes hayan hecho con terceros, en referencia al producto o servicio, o ambos, para aumentar la satisfacción del cliente.
- Mejorar la comunicación entre los proveedores, clientes y todas las partes interesadas en la cadena de entrega.
- Realizar evaluaciones de seguridad sobre la cadena de suministro, la cual desarrollara contramedidas adecuadas.

Todo lo anterior hace necesario aplicar cada una de las normas que integra la serie NTC-ISO 28000, con el fin de que la organización conozca sus procesos críticos y estratégicos en el desarrollo de su negocio, lo cual le confiere la capacidad de determinar qué operaciones preventivas se deben realizar, con qué medios y recursos cuentan y deben contar, y en qué plazos se ejecutarán.

Esta publicación que se pone a disposición de las empresas colombianas tiene como propósito brindar a los empresarios colombianos todas las herramientas relacionadas con este tema de particular interés y actualidad.

Fabián Leonardo Colorado
Profesional de normalización
ICONTEC

NORMA TÉCNICA COLOMBIANA NTC-ISO 28000

2008-11-26

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

ICONTEC

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

PROLOGO

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

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

3M COLOMBIA
ABBOTT LABORATORES DE COLOMBIA S.A.
ACCIÓN SOCIAL - PRESIDENCIA DE LA REPÚBLICA
ACERÍAS DE CALDAS S.A.
ACERÍAS DE COLOMBIA -ACESCO-
ACUAVIVAS.A. E.S.P.
ACUEDUCTO DE BOGOTÁ
ALCALDÍA MUNICIPAL DE CALI
ALDÍA LOGÍSTICA
ALFA SERVICIOS DE GESTIÓN EMPRESARIAL
ALIMENTOS KRAFT
ALKOSTO
ALMACENAR
ALMACENES ÉXITO
ALTHVIZ & CÍA. LTDA.
ANALDEX
ASESORÍAS TÉCNICAS CORREDORES 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 DISTRIBUIDORESDE 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 CERTIFICARON
Cl. DE AZÚCARES Y MIELES S.A.
Cl. DISAN S.A.
CAFAM
CAJA DE COMPENSACIÓN FAMILIAR -COMPENSAR-
CAJAS Y SUPLEMENTOS
CÁMARA DE COMERCIO DE CALI
CAMIONES Y REMOLQUES LTDA. GARULLA
CARVAJAL S.A.
CASA LUKER S.A.
CENTELSA
CENTRALES DE TRANSPORTES S.A.
CENTRORIENTE S.A.
CHALLENGER
CHALLENGER S.A.
CÍA 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 DISTRIBUCCIÓÑ 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
CREDIBANCOVISA
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
LUMINEXS.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
TRANSPORTADORACOMERCIAL 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 & CÍA. LTDA. TRANSPORTES MULTIGRANEL S.A. TRANSPORTES PREMMIER LTDA. TRANSPORTES SIVAL

TRANSPORTES TERRESTRES DE CARGA LTDA.
TRANSPORTES VIGÍA S.A.
TRANSPORTES VILLAGÓMEZ LTDA.
TRANSPORTES Y SERVICIOS LTDA. -TRANSER LTDA.-
UNIAGRAR1A
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

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.

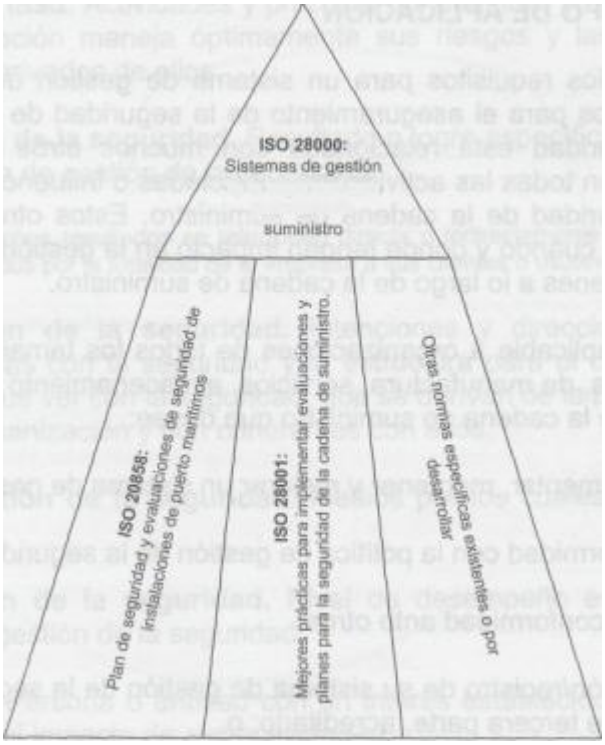

Figura 1. Relación entre la ISO 28000 y otras normas pertinentes

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 específica 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 Segundad. 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

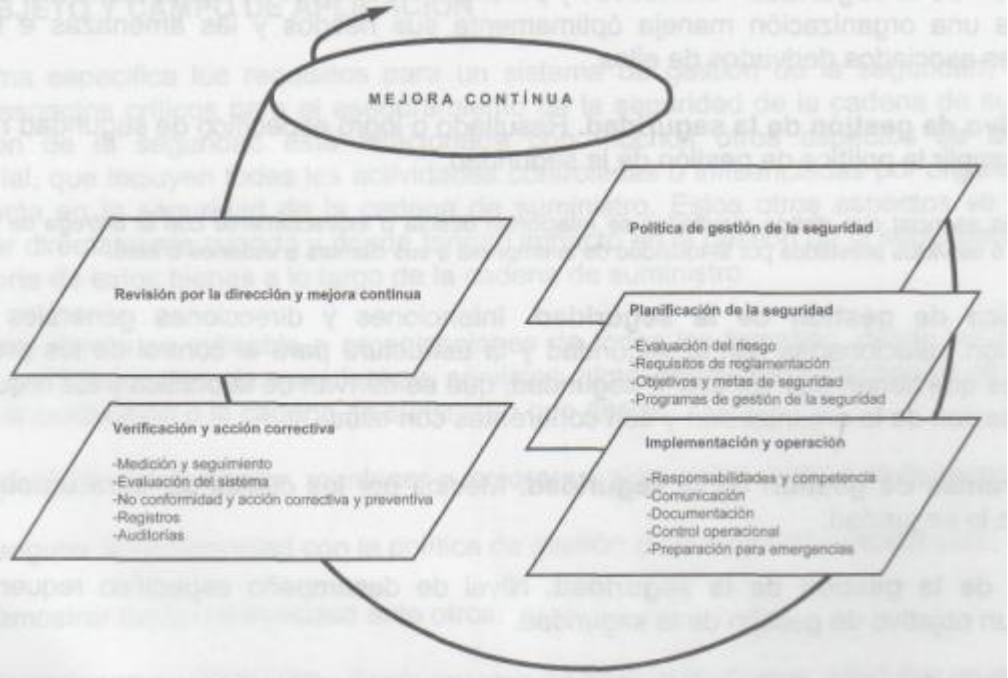

Figura 2. Elementos del sistema de gestión de la seguridad

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 segundad 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 segundad;

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 segundad 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 segundad;

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 segundad, 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		1509001:2000	
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

(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 STANDARDIZARON. *Specification for Security Management Systems forthe Supply Chain.* Geneva, Switzerland, ISO: 28000: 2007(E), p 16.

NORMA TÉCNICA COLOMBIANA NTC-ISO 28001

2008-11-26

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO. MEJORES PRÁCTICAS PARA IMPLEMENTAR EVALUACIONES Y PLANES PARA LA SEGURIDAD DE LA CADENA DE SUMINISTRO. REQUISITOS Y ORIENTACIÓN

ICONTEC

E: SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN. BEST PRACTICES FOR IMPLEMENTIN SUPPLY CHAIN SECURITY. ASSESSMENTS AND PLANS.REQUIREMENTS AND GUIDANCE

CORRESPONDENCIA: esta norma es una adopción idéntica por traducción (IDT), respecto al documento de referencia, la norma ISO 28001.

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 28001 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.

ALMAGRAN S.A.
ALPINA S.A.
ASOCIACIÓN COLOMBIANA DE EMPRESAS CARROCERAS -ASCECAR-
AXONICA
Cl. DISAN S.A.
CARROCERÍAS BENFOR
CARROCERÍAS EL SOL
COLFECAR
COLSEGUROS
COLTANQUES
ICOLLANTAS
INLAC
METROPYME
QUALITAS INGENIERÍA
SERVIENTREGA S.A.
SOANSES LTDA.
SOCIEDAD TRACTEC
TITADSU
TRANSPORTE BOTERO SOTO
VALENTINA S.A.

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

3M COLOMBIA
ABBOTT LABORATORES DE COLOMBIA S.A.
ACCIÓN SOCIAL -PRESIDENCIA DE LA REPÚBLICA-
ACERÍAS DE CALDAS S.A.
ACERÍAS DE COLOMBIA -ACESCO-
ACUAVIVAS.A. E.S.P
ACUEDUCTO DE BOGOTÁ
ALCALDÍA MUNICIPAL DE CALI
ALDÍA LOGÍSTICA
ALFA SERVICIOS DE GESTIÓN EMPRESARIAL
ALIMENTOS KRAFT
ALKOSTO
ALMACENAR
ALMACENES ÉXITO
ALMACENES GENERALES DE DEPÓSITO GRAN COLOMBIA S.A. -ALMAGRAN-
ALPINA S.A.
ALTHVIZ & CÍA. LTDA.
ANALDEX
ASESORÍAS TÉCNICAS CORREDORES 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-
ASOCIACION NACIONAL DE TRANSPORTADORES -ASOTRANS-
ASOCIADOS DISTRIBUIDORES DE DERIVADOS DEL PETRÓLEO -ADISPETROL-
ATENCIÓN TÉCNICA EN CALIDAD LTDA.
AUTOAIRESS..A.
AUTO FUSA S.A.
AVON
BAVARIA S.A.
BEC INTERNATIONAL LTDA.
BUREAU VERITAS CERTIFICARON
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.
GARULLA
CARVAJAL S.A.
CASA LUKER S.A.
CENTELSA
CENTRALES DE TRANSPORTES S.A.
CENTRORIENTE S.A.
CHALLENGER S.A.
CÍA COLOMBIANA DE TRANSPORTES S.A. -COLDETRANS S.A.-
CLÍNICA DE OCCIDENTE S.A.
COCA-COLA -PANAMCO COLOMBIA S.A.-
COLCERÁMICA
COLGATE PALMOLIVE
COLOMBIANA DE TANQUES LTDA. -COLTANQUES LTDA-
COLOMBIANA KIMBERLY COLPAPEL S.A.
COMFAMA
COMFENALCO SANTANDER
COMPAÑÍA COLOMBIANA AUTOMOTRIZ
COMPAÑÍA DE CARGA MOVITRANSPORTES LTDA.
COMPAÑÍA DE DISTRIBUCCIÓN 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 DELSURCOTRASUR
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
CRÉDIBANCOVISA
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
LUMINEXS.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.
NESTLÉ 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 & CÍA. LTDA. TRANSPORTES MULTIGRANEL S.A. TRANSPORTES PREMMIER LTDA. TRANSPORTES SIVAL TRANSPORTES TERRESTRES DE CARGA LTDA. TRANSPORTES VIGÍA 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

INTRODUCCIÓN

Los incidentes de seguridad contra cadenas de suministro internacionales son amenazas para el comercio internacional y el crecimiento económico de las naciones que comercian. Es necesario proteger el personal, los bienes, la infraestructura y los equipos, incluidos los medios de transporte, contra incidentes de seguridad y sus efectos potencialmente devastadores. Esta protección beneficia a la economía y a la sociedad en general.

Las cadenas de suministro internacionales son muy dinámicas y están compuestas de muchas entidades y socios comerciales. La presente norma reconoce esta complejidad; ha sido desarrollada para permitir que una organización individual dentro de la cadena de suministro aplique sus requisitos de conformidad con el modelo de negocio particular de la organización y su rol y función en la cadena de suministro internacional.

Esta norma brinda una opción para que las organizaciones establezcan y documenten niveles razonables de seguridad dentro de las cadenas de suministro internacionales y sus componentes. Posibilitará que estas organizaciones tomen mejores decisiones basadas en el riesgo, concernientes a la seguridad en estas cadenas de suministro internacionales.

La presente norma es multimodal y está prevista para ser utilizada conjuntamente con el Marco de Estándares de la Organización Mundial de Aduanas y para complementarlo, con el fin de asegurar y facilitar el comercio global (estructura). No pretende abarcar, reemplazar ni sustituir los programas de seguridad de la cadena de suministro de las agencias de aduanas individuales ni sus requisitos de certificación y validación.

El uso de esta norma ayudará a que una organización establezca sus niveles adecuados de seguridad dentro de las partes de la cadena de suministro internacional que controla. También es una base para determinar o validar el nivel de segundad existente dentro de las cadenas de suministro de estas organizaciones, por parte de auditores internos y externos o por las agencias gubernamentales que deciden usar la conformidad con esta norma como la línea de referencia para la aceptación en sus programas de seguridad de la cadena de suministro. Los clientes, socios comerciales, agencias gubernamentales y otros podrían solicitar que las organizaciones que declaren conformidad con esta norma sean sometidas a una auditoría o validación para confirmar dicha conformidad. Las agencias gubernamentales podrían acordar mutuamente aceptar validaciones realizadas por otras agencias gubernamentales. Si se va a llevar a cabo una auditoría a una organización, por una tercera parte, la organización debe considerar que se contrate un organismo de certificación de tercera parte acreditado por un organismo competente que sea miembro del Foro Internacional de Acreditación (véase el Anexo C).

Con esta norma no se pretende duplicar los requisitos y normas gubernamentales concernientes a la seguridad de la cadena de suministro de conformidad con el marco SAFE de la OMA. Las organizaciones que ya han sido certificadas o validadas por gobiernos que se reconocen mutuamente, cumplen con esta norma.

Las salidas de esta norma serán las siguientes:

- Una Declaración de Cobertura que defina los límites de la cadena de suministro cubierta por el plan de seguridad.

- Una evaluación de seguridad que documente la vulnerabilidad de la cadena de suministro a escenarios de amenaza para la seguridad definidos. También describe los impactos que se pueden esperar razonablemente de cada escenario potencial de amenaza para la seguridad.

- Un plan de seguridad que describa las medidas de seguridad implementadas para manejar los escenarios de amenaza para la seguridad identificados mediante la evaluación de la seguridad.

- Un programa de entrenamiento que establezca cómo se entrenará al personal de seguridad para que cumpla sus deberes asignados relacionados con la segundad.

Para llevar a cabo la evaluación de seguridad necesaria para elaborar el plan de seguridad, una organización que use esta norma:

- Identificará las amenazas planteadas (escenarios de amenaza para la seguridad);

- Determinará la posibilidad con que las personas pueden evolucionar cada uno de los escenarios de amenazas a la seguridad identificados mediante la evaluación de la seguridad hacia un incidente de seguridad.

Esta determinación se hace revisando el estado actual de la seguridad en la cadena de suministro. Con base en los hallazgos de esta revisión, se usa el criterio profesional para identificar la vulnerabilidad de la cadena de suministro con cada escenario de amenaza a la seguridad.

Si la cadena de suministro se considera inaceptablemente vulnerable a un escenario de amenaza a la seguridad, la organización desarrollará procedimientos adicionales o cambios operacionales para reducir la posibilidad, la consecuencia, o ambas. Estas se denominan contramedidas. Con base en un sistema de prioridades, las contramedidas se deben incorporar al plan de seguridad para reducir la amenaza a un nivel aceptable.

Los Anexos A y B presentan ejemplos ilustrativos de procesos de seguridad basados en gestión del riesgo, para proteger a las personas, activos y misiones de la cadena de suministro internacional. Facilitan un enfoque macro para las cadenas de suministro complejas, o enfoques más discretos para porciones de ellas, o ambos.

Estos anexos también pretenden:

- facilitar la comprensión, adopción e implementación de metodologías que pueden ser adaptadas por las organizaciones;

- brindar orientación para gestión de la seguridad de referencia, para la mejora continua;

- ayudar a las organizaciones a gestionar recursos para abordar los riesgos para la seguridad existentes y los emergentes;

- describir los posibles medios de evaluar el riesgo y mitigar las amenazas a la seguridad en la cadena de suministro, desde la asignación de la materia prima pasando por el almacenamiento, fabricación y transporte de los productos terminados hasta el mercado.

El Anexo C proporciona orientación para la obtención de asesoría y certificación con esta norma, si una organización elige esta opción.

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO. MEJORES PRÁCTICAS PARA IMPLEMENTAR EVALUACIONES Y PLANES PARA LA SEGURIDAD DE LA CADENA DE SUMINISTRO. REQUISITOS Y ORIENTACIÓN

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma presenta requisitos y orientación para organizaciones en cadenas de suministro internacionales, de manera que éstas:

- desarrollen e implementen procesos de seguridad de la cadena de suministro;
- establezcan y documenten un nivel mínimo de seguridad dentro de una(s) cadena(s) de suministro o segmento de ésta;
- ayuden a cumplir los criterios del Operador Económico Autorizado (OEA) establecidos en el Marco de Estándares de la Organización Mundial de Aduanas y cumplir los programas de seguridad de la cadena de suministro nacional.

NOTA Solamente una Agencia de Aduanas Nacional participante puede designar organizaciones como OEA de acuerdo con su programa de seguridad de la cadena de suministro y sus requisitos de certificación y validación relacionados.

Además, la presente norma establece algunos requisitos de documentación que permitirían la verificación.

Los usuarios de esta norma:

- definirán la parte de una cadena de suministro internacional dentro de la cual han establecido seguridad (véase el numeral 4.1);
- realizarán evaluaciones de seguridad sobre esa parte de la cadena de suministro y desarrollarán contramedidas adecuadas;
- desarrollarán e implementarán un plan de seguridad de la cadena de suministro; entrenarán al personal de seguridad en sus deberes relacionados con la seguridad.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos normativos referenciados son indispensables para la aplicación de este documento normativo. Para referencias fechadas, se aplica únicamente la edición citada.

Para referencias no fechadas, se aplica la última edición del documento normativo referenciado (incluida cualquier corrección).

ISO 20858, Ships and Marine Technology. Maritime Port Facility Security Assessments and Securíty Plan Development

International Convention for the Safety of Life at Sea (SOLAS), 1974, corregida, International Maritime Organizaron.

3. TÉRMINOS Y DEFINICIONES

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

3.1 Funcionarios que vigilan la aplicación de la ley y otros funcionarios de gobierno apropiados. Personal del gobierno y personal que vigila la aplicación de la ley, que tiene jurisdicción legal específica sobre la cadena de suministro internacional o partes de ella.

3.2 Activo(s). Plantas, maquinaria, propiedades, edificaciones, vehículos, barcos, aeronaves, transportes y otros elementos de infraestructura, o plantas y sistemas relacionados que tienen una función o servicio para el negocio definidos y cuantificables.

NOTA Esta definición incluye cualquier sistema de información que sea integral a la entrega de seguridad y a la aplicación de la gestión de la seguridad.

3.3 Operador Económico Autorizado (OEA). Parte involucrada en el movimiento internacional de bienes, en cualquier función que haya sido aprobada por una administración nacional de aduanas o en nombre de ésta, de conformidad con la OMA (Organización Mundial de Aduanas) o normas de seguridad de la cadena de suministro equivalentes.

NOTA 1 Operador económico autorizado es un término que se encuentra definido en el Marco de Estándares de la Organización Mundial de Aduanas.

NOTA 2 Los operadores económicos autorizados incluyen, entre otros, fabricantes, importadores, exportadores, corredores, transportadores, consolidadores, intermediarios, puertos, aeropuertos, operadores integrados, bodegas y distribuidores.

3.4 Socio comercial Los contratistas, proveedores de productos o servicios que una organización contrata para ayudar a una organización en su función como **organización de la cadena de suministro** (véase el numeral 3.15).

3.5 Unidad de transporte de carga. Vehículo para transporte de carga por carretera, vagón de carga, contenedor de carga, carrotanque, vagón para transporte de líquidos, o tanque portátil.

3.6 Consecuencia. Pérdida de la vida, daño a la propiedad o trastornos económicos, incluidos trastornos en los sistemas de transporte, que se pueden esperar razonablemente como resultado de un ataque a una organización de la cadena de suministro, o por el uso de la cadena de suministro como un arma.

3.7 Transporte. Instrumento físico de comercio internacional para enviar carga de un lugar a otro.

EJEMPLOS Caja, estiba, unidad de transporte de carga, equipo para manipulación de carga, camión, barco, avión y ferrocarril.

3.8 Contramedidas. Acciones tomadas para reducir la posibilidad de que un escenario de amenaza para la seguridad tenga éxito en sus objetivos, o para reducir las posibles
consecuencias de un escenario de amenazas a la seguridad.

3.9 Custodia. Período de tiempo en el que una organización en la cadena de suministro está controlando directamente la fabricación, proceso, manipulación y transporte de mercancías, y la información relacionada con su despacho dentro de la cadena de suministro.

3.10 Aguas abajo. Manipulación, procesos y movimientos de mercancías cuando ya no están en la custodia de la organización en la cadena de suministro.

3.11 Mercancías. Elementos o materiales que, una vez que se coloca una orden de compra, son fabricados, procesados, manipulados o transportados dentro de la cadena de suministro para uso o consumo por parte del comprador.

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

NOTA 1 Todas las partes de esta cadena se consideran internacionales desde el momento en que se concluye la orden de compra, hasta el punto en que las mercancías salen del control de aduanas en el país o economía de destino.

NOTA 2 Si los tratados o acuerdos regionales han eliminado el despacho aduanero de mercancías desde países o economías especificadas, el final de la cadena de suministro internacional es el puerto de entrada al país o economía de destino en donde las mercancías habrían pasado por la aduana si no hubiera acuerdos o tratados.

3.13 Posibilidad. Facilidad o dificultad con la cual un escenario de amenazas a la seguridad podría progresar para llegar a ser un incidente de seguridad.

NOTA La posibilidad se evalúa con base en la resistencia que los procesos de seguridad oponen a un incidente de seguridad que involucra el escenario de amenazas que se examinan, y se expresa cualitativa o cuantitativamente.

3.14 Sistema de gestión. La estructura de la organización para manejar sus procesos o actividades que transforman entradas de recursos en un producto o servicio, que cumple los objetivos de la organización.

NOTA Esta norma no pretende especificar un sistema de gestión de la calidad específico, ni exigir la creación de un sistema de gestión de la seguridad separado. Algunos ejemplos de sistemas de gestión son la norma ISO 9001 (Sistemas de gestión de la calidad), la norma ISO 140001 (Sistemas de gestión ambiental), la norma ISO 28000 (sistemas de gestión de seguridad para la cadena de suministro) y el Código para gestión de seguridad internacional de las organizaciones marítimas internacionales) (ISM).

3.15 Organización de la cadena de suministro. Entidad que:

- Al ser colocada una orden de compra, fabrica, maneja, procesa, carga, consolida, descarga o recibe mercancías que en algún punto cruzan una frontera internacional o económica.
- Transporta mercancías por cualquier medio en la cadena de suministro internacional, independientemente de si su segmento particular de la cadena de suministro cruza fronteras nacionales (o económicas), o
- Suministra, gestiona o dirige la generación, distribución o flujo de información de despacho usada por las agencias de aduanas o en las prácticas comerciales.

3.16 Gestión del riesgo. Proceso de tomar decisiones basadas en el análisis de posibles amenazas, sus consecuencias y su probabilidad o posibilidad de éxito.

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

3.17 Alcance del servicio. Funciones que realiza una organización en la cadena de suministro, y el lugar en donde realiza estas funciones.

3.18 Declaración de seguridad. Compromiso documentado por un socio comercial, que especifica las medidas de seguridad implementadas por él, que incluye, como mínimo, cómo se protegen las mercancías e instrumentos físicos del comercio internacional, cómo se protege la información asociada y se demuestran y verifican las medidas de seguridad.

NOTA La organización en la cadena de suministro la utilizará para evaluar la conveniencia de las medidas relacionadas con la seguridad de las mercancías.

3.19 Plan de seguridad. Disposiciones planificadas para garantizar que la seguridad se maneja en forma adecuada.

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

NOTA 2 El plan puede estar incorporado en otros planes operacionales.

3.20 Seguridad. Resistencia a actos intencionales destinados a causar daño o perjuicio a la cadena de suministro, o por ella.

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

3.22 Personal de seguridad. Personas en la organización, en la cadena de suministro, a quienes se ha asignado deberes relacionados con la segundad.

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

3.23 Información de seguridad confidencial - Materiales de seguridad confidenciales. Información o materiales producidos o incluidos en el proceso de seguridad de la cadena de suministro, que contienen información acerca de los procesos de seguridad, despachos o directivas del gobierno que no estarían disponibles fácilmente para el público y serían útiles para alguien que desee iniciar un incidente de seguridad.

3.24 Cadena de suministro. Conjunto enlazado de recursos y procesos que comienza al colocarse una orden de compra, con el suministro de materia prima, y se extiende a la fabricación, procesamiento, manipulación y despacho de mercancías y servicios relacionados, al comprador.

NOTA La cadena de suministro puede incluir a los vendedores, instalaciones de fabricación, proveedores logísticos, centros de distribución interna, distribuidores, mayoristas y otras instancias involucradas en la fabricación, procesamiento, manipulación y despacho de mercancías y sus servicios relacionados.

3.25 Meta. Personal, medios de transporte, mercancías, activos físicos, procesos de fabricación, manipulación, sistemas de control o documentación dentro de una organización de la cadena de suministro.

3.26 Escenario de amenazas a la seguridad. Medio por el cual podría ocurrir un incidente de seguridad potencial.

3.27 **Aguas arriba.** Manipulación, procesos y movimientos de mercancías que ocurren antes de que la organización de la cadena de suministro asuma la custodia de las mercancías.

3.28 Organización Mundial de Aduanas (OMA). Organismo intergubernamental independiente cuya misión es mejorar la eficacia y eficiencia de las administraciones aduaneras.

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

4. CAMPO DE APLICACIÓN

4.1 DECLARACIÓN DE APLICACIÓN

La organización en la cadena de suministro debe describir en una "Declaración de aplicación" la parte de la cadena de suministro internacional con la que declara cumplimiento, con base en esta norma. La "Declaración de Aplicación" debe incluir al menos la siguiente información:

a) Detalles de la organización.

b) Alcance del servicio.

c) Nombres e información de contacto de todos los socios comerciales, dentro del alcance definido del servicio.

d) La fecha en que se finalizó la evaluación de seguridad y el período de validez de dicha evaluación, y

e) La firma de un individuo autorizado para firmar en nombre de la organización.

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

4.2 SOCIOS COMERCIALES

Si dentro de la cadena de suministro descrita en la Declaración de Aplicación la organización cuenta con socios comerciales, debe, de acuerdo con los numerales 4.3 y 4.4, exigir a dichos socios comerciales que suministren una declaración de seguridad. La organización debe considerar esta declaración de seguridad en su evaluación de la seguridad, y puede exigir que se promulguen contramedidas específicas.

4.3 CERTIFICADOS O APROBACIONES ACEPTADAS INTERNACIONALMENTE

Las compañías e instalaciones de transporte que tienen certificados o aprobaciones aceptadas internacionalmente, expedidas de acuerdo con convenciones internacionales obligatorias que gobiernan la seguridad de diversos sectores del transporte, tendrán implementados planes, prácticas y procesos de seguridad que cumplen los requisitos aplicables de la presente norma, y no se les exige auditorías para confirmar dicha conformidad. Para las compañías de transporte, barcos e instalaciones portuarias, los certificados o aprobaciones se deben expedir de acuerdo con SOLAS XI-2/4 ó SOLAS XI-2/10, según el caso.

De conformidad con el numeral 1, las agencias aduaneras nacionales, además de poseer certificaciones o aprobaciones de seguridad aceptadas internacionalmente, pueden exigir que las compañías e instalaciones de transporte tengan implementadas medidas y prácticas de seguridad adicionales, como condición para su designación como AEO.

4.4 SOCIOS COMERCIALES EXENTOS DEL REQUISITO DE DECLARACIÓN DE SEGURIDAD

Los socios comerciales que confirmen a la organización que:

a) Se ha verificado su conformidad con esta norma o con la ISO 20858.

b) Están comprendidos en el numeral 4.3, ó

c) Han sido designados como AEO de acuerdo con el programa de seguridad de la cadena de suministro de la agencia nacional de aduanas, que se ha determinado que está de acuerdo con el marco SAFE de la OMA.

Se deben incluir en la Declaración de Aplicación. Sin embargo, la organización no necesita realizar evaluaciones de seguridad adicionales para estos socios comerciales, ni pedirles que suministren declaraciones de seguridad.

4.5 REVISIONES DE SEGURIDAD DE LOS SOCIOS COMERCIALES

Excepto para los socios comerciales que se encuentran incluidos en los numerales 4.3 ó 4.4, la organización en la cadena de suministro debe llevar a cabo revisiones de los procesos e instalaciones de sus socios comerciales para determinar la validez de sus declaraciones de seguridad. El alcance y frecuencia de estas revisiones se debe determinar por medio de un análisis de los riesgos involucrados. La organización debe conservar los resultados de estas revisiones.

NOTA Con el fin de facilitar la lectura, la organización que declara conformidad, incluidas aquellas partes de su cadena de suministro operadas por socios comerciales, ya sea que cumplan con esta norma o no, en los párrafos siguientes mencionados se denominará la "organización" a menos que por claridad se requiera de otra manera.

5. PROCESO DE SEGURIDAD DE LA CADENA DE SUMINISTRO

5.1 GENERALIDADES

Las organizaciones en las cadenas de suministro internacionales que han adoptado esta norma deben tanto manejar la seguridad en toda la parte de la cadena de suministro que les corresponde, y contar con un sistema de gestión implementado, como soporte de este objetivo. Esta norma exige que se establezcan e implementen prácticas o procesos de seguridad, o ambos, con el fin de reducir el riesgo que tienen para la cadena de suministro internacional las actividades que puedan conducir a un incidente de seguridad.

Las organizaciones de la cadena de suministro que declaran conformidad con esta norma deben contar con un plan de seguridad basado en los resultados de la evaluación de seguridad, que documente las medidas y procedimientos de seguridad existentes, e incorpore contramedidas aplicables al (los) elemento(s) de la cadena de suministro internacional que han incluido en su Declaración de Aplicación.

5.2 IDENTIFICACIÓN DEL ALCANCE DE LA EVALUACIÓN DE LA SEGURIDAD

El alcance de la evaluación de la seguridad debe incluir todas las actividades realizadas por la organización, como se describe en la Declaración de Aplicación (véase el numeral 4.1). La evaluación se debe llevar a cabo periódicamente y el plan de seguridad se debe actualizar, según sea apropiado. Los resultados de la evaluación se deben documentar y conservar.

La evaluación de la seguridad también debe comprender los sistemas de información, los documentos y las redes relativas a la manipulación y movimiento de mercancías mientras están bajo custodia de la organización. Las disposiciones de seguridad existentes deben, sujetas a los numerales 4.3 y 4.4, ser evaluadas en todos los lugares y para socios comerciales en donde haya vulnerabilidad potencial a la seguridad.

5.3 REALIZACIÓN DE LA EVALUACIÓN DE LA SEGURIDAD

5.3.1 Personal de evaluación

La persona o equipo que lleva a cabo la evaluación de la seguridad debe contar, colectivamente, con las habilidades y el conocimiento que incluyen, entre otros:

- las técnicas de evaluación del riesgo aplicables a todos los aspectos de la cadena de suministro internacional desde el punto en donde la organización de la cadena de suministro asume la custodia de las mercancías, hasta el punto en donde éstas dejan de estar bajo la custodia de la organización o abandonan la cadena de suministro internacional;
- la aplicación de medidas apropiadas para evitar la divulgación o acceso no autorizados a material confidencial;
- las operaciones y procedimientos involucrados en la fabricación, manipulación, procesamiento, movimiento o documentación de mercancías, o todos ellos, según el caso;
- medidas de seguridad relacionadas con el despacho, transporte, personal, instalaciones y sistemas de información en esa parte aplicable de la cadena de suministro;

- entender las amenazas a la seguridad y de las metodologías de mitigación;

- entender esta norma.

Se debe(n) documentar el(los) nombre(s) de la(s) personas o miembros del equipo que llevan cabo la evaluación, al igual que sus calificaciones.

5.3.2 Proceso de evaluación

La organización debe establecer, implementar y mantener un(os) procedimiento(s) para identificar las contramedidas existentes para mitigar las amenazas a la seguridad. La organización debe elaborar una lista de escenarios de amenazas a la seguridad aplicables, incluidos los considerados necesarios por los funcionarios de gobierno apropiados. Si no han participado funcionarios del gobierno, esto se debe documentar en la evaluación de seguridad.

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

La organización debe revisar la(s) declaración(es) de seguridad suministrada(s) por cada socio comercial, definido en el numeral 4.2 y aplicar criterio profesional, el conocimiento de las entidades o los requisitos de las agencias de reglamentación, o todos ellos. También puede obtener y usar cualquier otra información disponible, al determinar la aceptación de la declaración.

Cuando se lleva a cabo la evaluación de la seguridad, las organizaciones deben considerar tanto los detalles como la validez de cada declaración de seguridad, y determinar la vulnerabilidad general de la cadena de suministro descrita en la Declaración de Aplicación.

No debería ser necesario evaluar adicionalmente a los socios comerciales que están incluidos en los numerales 4.3 ó 4.4:

Se debe documentar la siguiente información:

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

b) Los procesos usados al evaluar esas amenazas, y

c) Todas las contramedidas identificadas y priorizadas.

5.4 DESARROLLO DEL PLAN DE SEGURIDAD DE LA CADENA DE SUMINISTRO

Las organizaciones deben desarrollar y mantener un plan de seguridad para toda la parte de la cadena de suministro descrita en su Declaración de Aplicación. El plan puede ir separado en anexos, en donde cada uno de ellos describe la seguridad implementada para un segmento particular de la cadena de suministro, incluidas las medidas de seguridad que los socios comerciales de las organizaciones, de acuerdo con el numeral 4.3 ó 4.4, mantendrán de acuerdo con sus declaraciones de seguridad. El plan / los anexos también deben especificar cómo la organización haría seguimiento o revisaría periódicamente estas declaraciones de seguridad.

Las organizaciones deben revisar y considerar el uso de la orientación en los Anexos informativos A y B, cuando desarrollan sus planes de seguridad.

5.5 EJECUCIÓN DEL PLAN DE SEGURIDAD DE LA CADENA DE SUMINISTRO

La organización debe establecer un sistema de gestión que posibilite la implementación de procesos de segundad específicos de la cadena de suministro.

5.6 DOCUMENTACIÓN Y SEGUIMIENTO DEL PROCESO DE SEGURIDAD DE LA CADENA DE SUMINISTRO

5.6.1 Generalidades

La organización debe establecer y mantener procedimientos para documentar, hacer seguimiento y medir el desempeño de su sistema de gestión con referencia a lo anterior. La organización debe llevar a cabo auditorías del sistema de gestión a intervalos planificados, para asegurar que se han implementado y mantenido apropiadamente. Los resultados de las auditorías se deben documentar y retener.

5.6.2 Mejora continua

La organización debe evaluar las oportunidades de mejorar sus disposiciones de seguridad, como un medio para mejorar la seguridad de esta parte de la cadena de suministro.

5.7 ACCIONES REQUERIDAS DESPUÉS DE UN INCIDENTE DE SEGURIDAD

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

a) Determinar la causa del incidente y la acción correctiva.

b) Determinar la eficacia de las medidas y procedimientos para recuperación de la seguridad, y

c) Considerar estas determinaciones, reevaluar estas partes de la cadena de suministro de acuerdo con el numeral 5.3.2.

En el evento de una violación a la seguridad, la organización debe seguir procedimientos de reporte a las agencias aduaneras o a las agencias apropiadas que vigilan la aplicación de la ley, según el caso, y como se especifica en el plan de segundad y en las relaciones contractuales.

La organización debe retener los datos sobre los despachos y sobre la cadena de suministro requeridos, dentro de los límites de tiempo establecidos en las leyes y reglamentos aplicables.

5.8 PROTECCIÓN DE LA INFORMACIÓN DE SEGURIDAD

Los planes, medidas, procesos, procedimientos y registros de la organización se deben considerar información de seguridad confidencial y protegida contra acceso o divulgación no autorizada. Esta información se debe revelar únicamente a los individuos que "necesitan conocerla". Además de los funcionarios que vigilan el cumplimiento de la ley, o las personas designadas por ellos, un individuo tiene "necesidad de conocer" cuando:

a) requiere acceso a información de seguridad confidencial específica para llevar a cabo actividades incluidas en el plan de seguridad;

b) está en entrenamiento para llevar a cabo actividades incluidas en el plan de seguridad;

c) la información es necesaria para que el individuo supervise a otros mediante la ejecución de actividades de seguridad incluidas en el plan de seguridad; o

d) pertenece a una parte, o actúa a nombre de una parte que, de acuerdo con una relación contractual con la organización, se le ha concedido acceso a información de seguridad controlada por la organización de acuerdo con los términos y condiciones establecidas.

NOTA Si la organización está certificada conforme con la norma ISO 28001 por una organización de certificación por tercera parte acreditada por un organismo de acreditación competente, o ha sido certificada o validada con la norma ISO 28001 por gobiernos que tienen acuerdos de reconocimiento mutuo, es posible que este acceso a la información confidencial de seguridad de la información, acordado contractualmente, no se considere necesario, y en cualquier evento dependería de la conformidad explícita de la organización. El hecho de que su información de seguridad confidencial esté protegida contra acceso o divulgación no autorizada no impide que la organización dé instrucciones a sus socios comerciales y a otros acerca de sus disposiciones y sistemas de seguridad de la cadena de suministro.

ANEXO A
(Informativo)

PROCESO DE SEGURIDAD DE LA CADENA DE SUMINISTRO

A.1 GENERALIDADES

Este anexo suministra información sobre el desarrollo de un proceso de la cadena de suministro que se puede implementar en una organización con el sistema de gestión existente. La Figura A.1 presenta una descripción gráfica de este proceso:

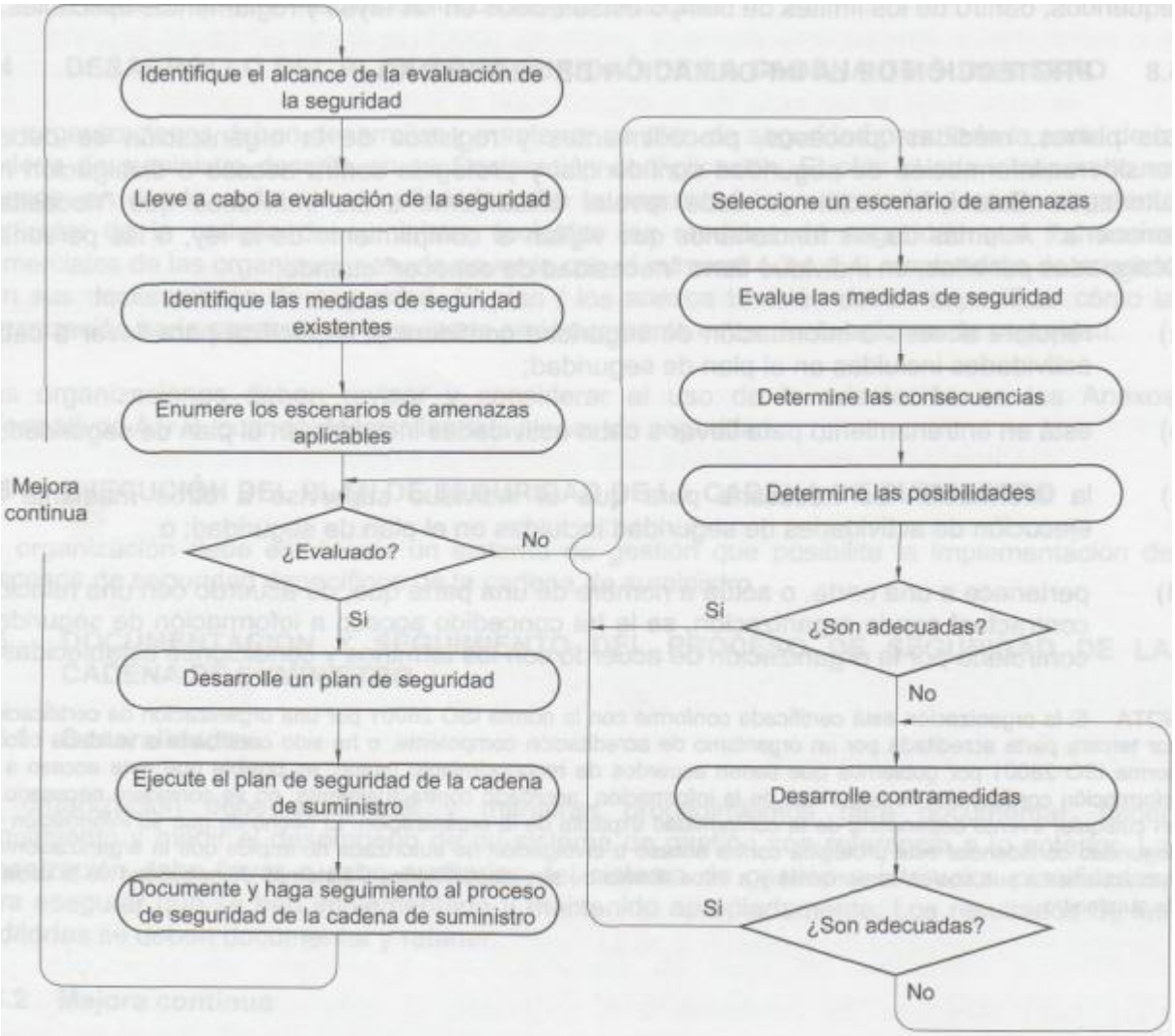

Figura A.1. Descripción gráfica de un proceso de seguridad de la cadena de suministro

A.2 IDENTIFICACIÓN DEL ALCANCE DE LA EVALUACIÓN DE LA SEGURIDAD

Una evaluación de la seguridad es un intento por identificar los riesgos de seguridad presentes en esa parte de la cadena de suministro, de acuerdo con su Declaración de Aplicación, que la organización desea llevar a cumplimiento con esta norma. Para lograr esta evaluación, es necesario establecer los límites del alcance de la cobertura (física y virtual).

A.3 REALIZACIÓN DE LA EVALUACIÓN DE LA SEGURIDAD

A.3.1 Generalidades

Utilizando personal calificado, se deben evaluar todas \as medidas de seguridad existentes en todos los lugares en donde hay vulnerabilidades potenciales a la seguridad, lo cual debería incluir, entre otros:

- El lugar en donde las mercancías son fabricadas, procesadas o manipuladas antes de ser cargadas en una unidad de transporte, en estibas, o preparadas de cualquier otra manera para el despacho.
- En donde las mercancías preparadas para despacho son almacenadas o consolidadas antes del transporte;
- En donde las mercancías son trasportadas.
- En donde las mercancías son cargadas o descargadas desde un medio de transporte;
- En donde la custodia de mercancías cambia de manos;
- En donde la documentación o información relativa a las mercancías que se despacha es manejada, generada o es accesible;
- Rutas de transporte nacionales y los medios usados por los diferentes medios de transporte;
- Otros.

A.3.2 Lista de revisión del desempeño

La siguiente lista de revisión del desempeño presenta un ejemplo de un enfoque sistemático para la revisión de las disposiciones de seguridad existentes.

Estas porciones de la lista de revisión del desempeño que corresponden a los socios comerciales, quienes han confirmado a la organización que:

a) Se ha verificado su conformidad con esta norma, o con la norma ISO 20858.

b) Está incluida por el numeral 4.3, ó

c) Ha sido designada como AEO de acuerdo con el programa de seguridad de la cadena de suministro de la agencia de aduanas nacional, que se ha determinado que está conforme con el marco SAFE de la OMA.

Deberían incluir un comentario que indique cómo se ha abordado el factor, por ejemplo, la conformidad con esta norma ISO 20858, o el Código ISPS.

A.3.3 Revisión del desempeño

La siguiente lista de revisión del desempeño en la Tabla A.1 se puede completar y considerar cuando se lleva a cabo una evaluación de segundad para una organización en la cadena de suministro. Esta lista no es exhaustiva y se puede adaptar para reflejar la evaluación del riesgo y el modelo de negocio de la organización. Si el factor indicado ya está implementado por la organización en la cadena de suministro, se debería marcar el recuadro "sí". Si el factor no está implementado todavía, o se cumple parcialmente, se debería marcar el recuadro "No", y en donde sea aplicable, se debería incluir una explicación en la columna de comentarios, que describa otras medidas alternativas utilizadas, o que el riesgo es muy bajo. Si el factor no es aplicable o está por fuera de la declaración de cobertura de la organización, en el recuadro "comentarios" se debería registrar "No Aplicable". Los elementos en la lista de revisión del desempeño que no se pueden ejecutar debido a las leyes/reglamentaciones aplicables, se deberían marcar como prohibidos en la columna de comentarios.

Tabla A.1. Lista de revisión del desempeño

Factor	Sí	No	Comentarios
Gestión de la seguridad de la cadena de suministro			
¿La organización cuenta con un sistema de gestión que tiene en cuenta la seguridad de la cadena de suministro?			
¿La organización cuenta con una persona designada como responsable de la seguridad de la cadena de suministro?			
Plan de seguridad			
¿La organización cuenta actualmente con un(os) plan(es) de seguridad?			
¿El plan tiene en cuenta las expectativas de seguridad de la organización de los socios comerciales aguas arriba y aguas abajo?			
¿La organización cuenta con un plan para manejo de crisis, continuidad del negocio y recuperación de la seguridad?			
Seguridad de los activos			
¿La organización ha implementado medidas que tengan en cuenta: la seguridad física de las edificaciones; el seguimiento y control de los perímetros exterior e interior; aplicación de controles de acceso que prohíben el acceso no autorizado a instalaciones, medios de transporte, plataformas de carga, áreas de carga y control administrativo, para la expedición de la identificación (empleados, visitantes, etc.) y otros dispositivos de acceso? ¿Existen tecnologías de seguridad operacional que incrementen significativamente la protección de los activos? Por ejemplo, detección de intrusos o cámaras de registro CCTV/DVS que comprenden áreas de importancia para la actividad de la cadena de suministro, y los registros se mantienen durante un período de tiempo suficientemente prolongado que se pueda usar en una investigación de un incidente.			
¿Se han implementado protocolos para contactar al personal de seguridad interna o al personal que vigila el cumplimiento de la ley, en caso de una violación a la seguridad?			
¿Se han implementado procedimientos para restringir, detectar y reportar acceso no autorizado a todas las áreas de almacenamiento de carga y medios de transporte?			
¿Las personas que entregan o reciben la carga se identifican antes de recibir o liberar la carga?			
Seguridad del personal			
¿La organización cuenta con procedimientos para evaluar la integridad de los empleados antes de su contratación y periódicamente, en relación con sus deberes de seguridad?			

Continúa. . .

Tabla A.1. Continuación

Factor	Sí	No	Comentarios
¿La organización lleva a cabo entrenamiento apropiado para los trabajos específicos, para ayudar a los empleados a ejecutar sus deberes de seguridad, por ejemplo: mantenimiento de la integridad de la carga, reconocimiento de las amenazas internas potenciales a la seguridad y protección de los controles de acceso?			
¿La organización informa a los empleados acerca de los procedimientos que ha implementado la compañía para reportar incidentes sospechosos?			
¿El sistema de control de acceso incluye el retiro inmediato de la identificación del empleado expedida por la compañía, cuando rescinde su contrato, y el retiro del acceso a áreas confidenciales y de sistemas de la información?			
Seguridad de la información			
¿ Los procedimientos empleados para asegurar que toda la información usada para el procesamiento de carga, tanto manual como electrónica, es legible, exacta y está protegida contra alteración, pérdida o introducción de datos erróneos?			
¿Una organización que despacha o recibe carga coteja la carga con la documentación de despacho apropiada?			
¿La organización se asegura de que la información de la carga recibida de los socios comerciales se reporte con exactitud y de una manera oportuna?			
¿Los datos pertinentes están protegidos mediante sistemas de almacenamiento no dependientes de la operación del sistema contra alteración de datos primarios (hay implementado un proceso para el respaldo de datos)?			
¿Todos los usuarios tienen un identificador único (ID del usuario) para su uso único y personal, para asegurar que se pueda hacer seguimiento a sus actividades?			
¿El sistema de gestión cuenta con una contraseña efectiva para autenticar a los usuarios, y estos deben cambiarla al menos una vez al año?			
¿Existe protección contra acceso no autorizado y la mala utilización de la información?			
Mercancías y seguridad en el transporte			
¿Hay implementados procedimientos para restringir, detectar y reportar acceso no autorizado a todas las áreas de despacho, plataformas de carga y almacenamiento de unidades de transporte de carga cerradas hasta el almacenamiento?			
¿Hay personas calificadas designadas para supervisar las operaciones de carga?			
¿Hay implementados procedimientos para notificar a las autoridades apropiadas que vigilan el cumplimiento de la ley, en casos en donde se detectan o se sospechan anomalías o actividades ¡legales por parte de la organización?			
¿Hay implementados procedimientos para asegurar la integridad de las mercancías / carga cuando se envían a otra organización (proveedor de transporte, centro de consolidación, instalación intermodal, etc.) en la cadena de suministro?			
¿Hay implementados procesos para rastrear los cambios en los niveles de amenaza a lo largo de las rutas de transporte?			
¿Se suministran reglas de seguridad, procedimientos u orientación a los operadores de transporte (por ejemplo, evitar las rutas peligrosas)?			
Unidades cerradas para transporte de carga			
(El marco SAFE de la OMA incluye un "Programa de Integridad del sello) descrito en el apéndice del Anexo 1, que establece procedimientos concernientes a la fijación y verificación de sellos de alta seguridad u otros dispositivos de detección contra alteración, o todos los anteriores. El personal que diligencie este formato debería revisar esta sección del Marco).			
Si se usa una unidad cerrada para transporte de carga, ¿existen procedimientos documentados para fijar y registrar sellos mecánicos de alta seguridad que cumplan el ISO/PAS 17712, u otros dispositivos de detección contra alteración, por parte de quienes introducen la carga en la unidad?			

Tabla A.1. Final

Factor	Sí	No	Comentarios
Si se usa una unidad sellada para transporte de carga, ¿se implementan procedimientos documentados para inspeccionar los sellos y detectar señales contra alteración cuando la custodia de los medios de transporte cambia durante el curso de un despacho, y para tener en cuenta las discrepancias detectadas?			
Factor			
Si se usa una unidad cerrada para transporte de carga, ¿es inspeccionada, por parte de quien introduce la carga, para determinar presencia de contaminación, inmediatamente antes de esta			
Si se usan unidades cerradas para transporte de carga, ¿se implementan procedimientos documentados para inspeccionarlas inmediatamente antes de que las personas encargadas introduzcan la carga, para verificar su integridad física, con el fin de incluir la confiabilidad de los mecanismos de bloqueo de la unidad? Se recomienda un proceso de inspección de siete puntos: Pared frontal. Lado izquierdo. Lado derecho. Piso. Techo/cielo raso. Cerramiento interior/exterior Exterior/tren de aterrizaje			

A.3.4 Escenarios de amenazas a la seguridad

Durante la evaluación de la seguridad considere los escenarios de amenazas a la seguridad, que incluyen, entre otros, los escenarios presentados en la Tabla A.2. La evaluación de la seguridad también debería considerar otros escenarios que pueden determinar las autoridades gubernamentales, la dirección de la organización o el(los) profesional(es) de seguridad que lleva(n) a cabo la evaluación.

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

Escenarios de amenazas a la seguridad	Aplicación
Entrometerse o tomar control, o ambos, de un activo (incluidos los medios de transporte) dentro de la cadena de suministro.	Daño/destrucción de un activo (incluidos los medios de transporte) Daño/destrucción por fuera de la meta usando los activos o mercancías. Provocar perturbaciones civiles o económicas Toma de rehenes/asesinatos
Uso de la cadena de suministro para actividades de contrabando.	Armas ilegales en el país o en la economía, o fuera de ellos. Terrorismo en el país / economía o fuera de él.

Continúa.

Escenarios de amenazas a \a seguridad	Aplicación
3. Alteración de la información	Se obtiene acceso local o remoto a los sistemas de información de documentación / información de la cadena de suministro, con el propósito de interrumpir las operaciones o facilitar actividades ilegales.
4. Integridad de la carga	Alteración, sabotaje o robo, o todas ellas, con fines terroristas.
5. Uso no autorizado	Realización de operaciones en la cadena de suministro internacional, para facilitar un incidente terrorista, incluido el uso del medio de transporte como arma.
6. Otro	

A.4 DESARROLLO DEL PLAN DE SEGURIDAD

A.4.1 Generalidades

El plan de seguridad o los anexos, o ambos, se puede(n) incorporar a los planes o procedimientos operativos, y no necesitan ser documentos independientes. Si el plan de seguridad está incorporado a otros planes, la organización debería mantener una tabla de referencia cruzada para posibilitar la verificación de que se han cumplido todos los requisitos del plan de seguridad.

El plan puede ir separado en anexos en los que se describe la seguridad implementada para un segmento particular de la cadena de suministro, incluidas las medidas que sus socios comerciales mantendrán de acuerdo con sus declaraciones de seguridad (si es aplicable). El plan / anexos también deberían especificar cómo la organización haría seguimiento o revisaría periódicamente sus declaraciones de seguridad. El plan / anexo de seguridad debería incluir, entre otras, descripciones de lo siguiente:

- La parte de la cadena de suministro que está incluida en el plan o anexo. Los

  deberes relacionados con la seguridad de todo el personal.
- La estructura de gestión de la seguridad, incluido el nombre de la persona designada como el director de seguridad.
- La información de contacto de seguridad de emergencia, interna y externa, que va a ser usada por el personal que reporta un incidente de seguridad.
- Las habilidades y conocimientos que el personal con responsabilidad de seguridad debe poseer.
- Programas de entrenamiento en seguridad.
- El proceso de calificación para el personal al que se ha asignado deberes de seguridad, que asegura que poseen las habilidades y el conocimiento necesarios para llevar a cabo sus deberes de seguridad.
- Cómo se ejecutan los elementos del plan de seguridad. La participación en prácticas de seguridad dirigidas por el gobierno o ejercicios por el personal de la organización se puede usar para cumplir estos requisitos.

- Procesos que deben cumplir, como mínimo, los requisitos de seguridad impuestos por el gobierno para contingencias o niveles de seguridad incrementados.

El plan de seguridad debería contener procedimientos que incluyan, entre otras, medidas para:

- Asegurar que la información sobre un despacho de mercancías sea recibida antes de que las mercancías que se despachan sean aceptadas por la organización para su transporte.
- Asegurar que las mercancías/cargas recibidas para consolidación / desconsolidación están cotejadas exactamente contra la información de los manifiestos/listas de mercancías/carga. Las unidades de carga/mercancías deben verificar contra las órdenes de compra o de despacho.
- Asegurar que los conductores que despachan o reciben mercancías/carga están positivamente identificados antes de recibir o enviar las unidades de carga o mercancías.
- Asegurar que los ocupantes de los vehículos, diferentes de los conductores, estén positivamente identificados.
- Asegurar que la falta, el exceso y otras discrepancias o anomalías significativas se resuelven o investigan apropiadamente, y que se notifica a las agencias apropiadas que vigilan el cumplimiento de la ley, si se detectan actividades ilegales o sospechosas, según sea apropiado.
- Describir cualquier contramedida que haya sido implementada en esa parte de la cadena de suministro.
- Describir cualesquier medidas y procedimientos que hayan sido implementados en esa parte de la cadena de suministro, para recuperación de la información en caso de un incidente de seguridad.
- Describir cualesquier medidas y procedimientos que hayan sido implementados cuando la custodia de las mercancías / carga se transfiere a otra organización.
- *Describir los procedimientos para emitir información adicional sobre las mercancías que son enviadas al personal autorizado. Estos deberían incluir cómo el usuario determinará si la solicitud de información adicional es legítima, qué información se emitirá, y de qué manera.*

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

A.4.2 Documentación

La organización debería mantener la documentación más reciente de la que se menciona a continuación, en un lugar seguro y en donde se pueda recuperar.

- Declaraciones de cobertura.

- Evaluación completa de la seguridad.

- Nombres y calificaciones del personal que lleva a cabo la evaluación de segundad.

- La lista de las contramedidas que se tuvieron en cuenta.
- Las declaraciones de seguridad.
- El plan de seguridad, y si es aplicable, los anexos.
- Registros de las sesiones de entrenamiento y los ejercicios realizados, el personal que asistió, los temas tratados y la(s) fecha(s).
- Otra, como se establece en los reglamentos, o por la dirección.

A.4.3 Comunicación

En donde sea viable, la organización debería establecer contacto con los funcionarios apropiados que vigilan el cumplimiento de la ley, y otros funcionarios gubernamentales, para los siguientes propósitos:

- Establecer procedimientos para seguir en caso de alteración de mercancía / carga, o sospecha de alteración de mercancía / carga, emergencias relacionadas con esto, o recibo de amenazas acerca de la cadena de suministro internacional. Estos procedimientos deberían incluir los números telefónicos específicos de las agencias gubernamentales a las que se debe llamar. Estos procedimientos se deberían incluir en el plan de seguridad de la cadena de suministro de la organización.
- Participar en consultas dirigidas por funcionarios gubernamentales apropiados tanto nacional como localmente (según el caso), para discutir asuntos de interés mutuo, incluidos los procedimientos y reglamentaciones aduaneras y los requisitos para la seguridad de las instalaciones y del despacho.
- Responder a los esfuerzos gubernamentales y contribuir al diálogo, que brinde un panorama significativo para asegurar que el plan de seguridad de las organizaciones sigue siendo pertinente y eficaz.

Si los funcionarios que vigilan el cumplimiento de la ley y otros funcionarios gubernamentales no desean participar en este diálogo, la organización debería documentar sus intenciones e indicar que los funcionarios que vigilan el cumplimiento de la ley y otros funcionarios gubernamentales, no desearon participar en ese momento.

A.5 EJECUCIÓN DEL PLAN DE SEGURIDAD

La implementación del plan de seguridad nuevo o actualizado representa un cambio en las prácticas operacionales y se debe emprender de acuerdo con el sistema de gestión de la organización para asegurar que se cuenta con los recursos suficientes, y que se haga seguimiento y evalúe el impacto sobre otras operaciones y la eficacia del plan.

A.6 DOCUMENTACIÓN Y SEGUIMIENTO DEL PROCESO DE SEGURIDAD

La organización debería establecer y mantener procedimientos para hacer seguimiento y medir el desempeño de su sistema de gestión de la seguridad, para asegurar su continua conveniencia, suficiencia y eficacia. La organización debería considerar las amenazas y riesgos a la seguridad asociados, incluidos los mecanismos de deterioro potencial y sus consecuencias, cuando se establece la frecuencia de la medición y del seguimiento de los parámetros de desempeño claves.

A.7 MEJORA CONTINUA

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

ANEXO B
(Informativo)

METODOLOGÍA PARA LA EVALUACIÓN DEL RIESGO DE LA SEGURIDAD Y DESARROLLO DE CONTRAMEDIDAS

B.1 GENERALIDADES

En este anexo se presenta la metodología que pueden usar las organizaciones en las cadenas de suministro internacionales para hacer una evaluación del riesgo de que sus operaciones pueden sufrir incidentes de seguridad, con el fin de determinar las contramedidas apropiadas y eficaces para el tipo y tamaño de las operaciones de su cadena de suministro. Esta *metodología utiliza la siguiente secuencia:*

a) Enumerar todas las actividades incluidas en el alcance.

b) Identificar los controles de seguridad implementados actualmente,

c) Identificar los escenarios de amenazas a la seguridad.

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

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

f) ¿Las medidas de control son suficientes?

g) Si no se han desarrollado medidas de seguridad adicionales.

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

B.2 PASO UNO. CONSIDERACIÓN DE LOS ESCENARIOS DE AMENAZA A LA SEGURIDAD

La evaluación de la seguridad debería considerar como mínimo los escenarios de amenaza a la seguridad enumerados en la Tabla B.1. La evaluación de la seguridad también debería considerar otros escenarios identificados por las autoridades gubernamentales, la gestión de la cadena de suministro o el profesional de seguridad que lleva a cabo la evaluación.

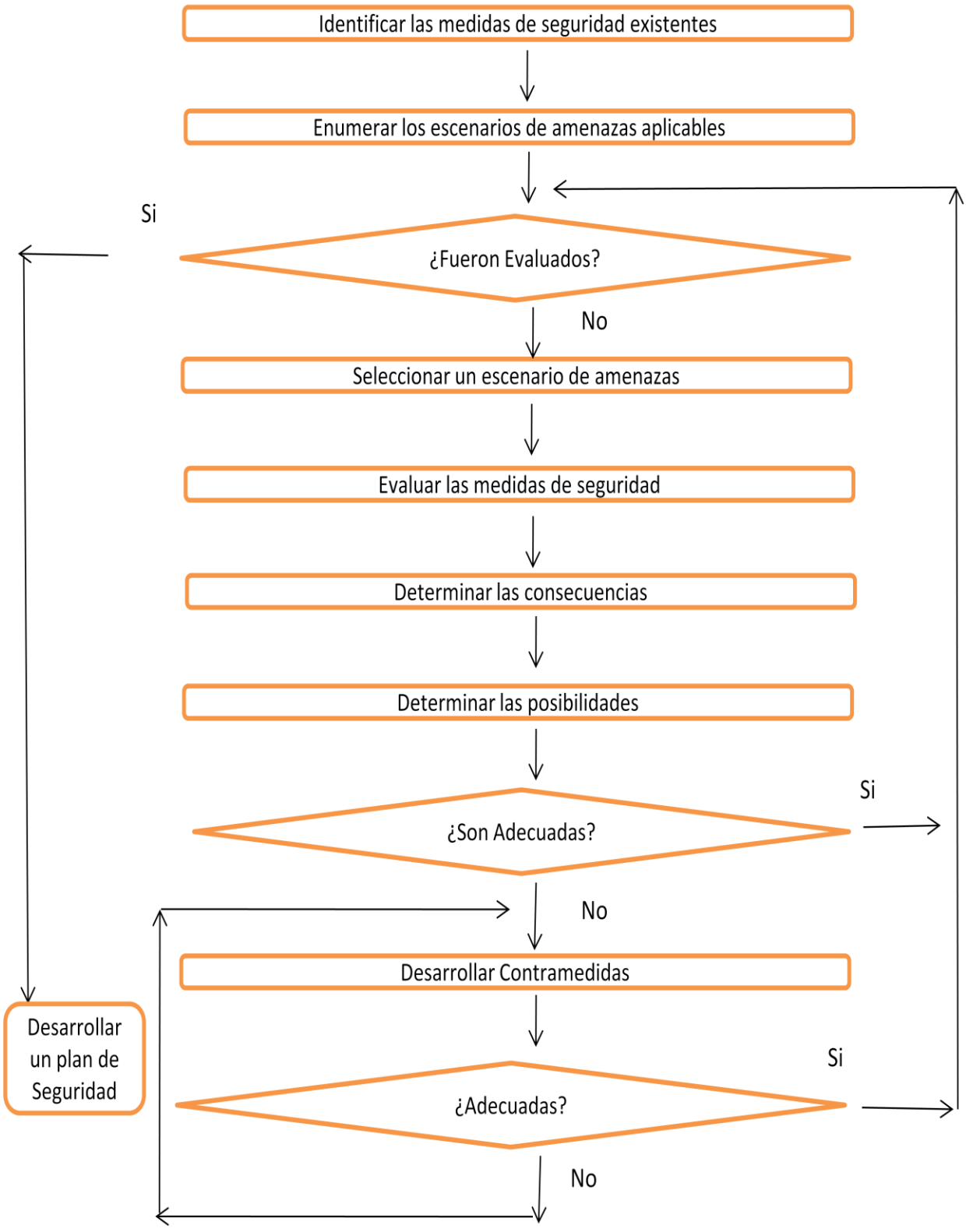

Figura B.1. Representación gráfica de una metodología para la evaluación del riesgo para la seguridad

Tabla B.1 Escenarios de amenaza a la seguridad de la cadena de suministro

Ejemplo de escenarios de amenaza a la seguridad	Ejemplo de aplicación
1 . Intromisión o toma del control de un activo, o ambos (incluidos los medios de transporte) dentro de la cadena de suministro	Daño/destrucción de un activo Daño/destrucción por fuera de la meta usando los activos o mercancías. Provocar perturbaciones civiles o económicas Toma de rehenes/asesinatos
2. Uso de la cadena de suministro como medio para acciones de contrabando	Armas ilegales en el país o en la economía. Terrorismo en el país/economía o fuera de él /ella.
3. Alteración de la información	Se obtiene acceso local o remoto a los sistemas de documentación / información de la cadena de suministro con el propósito de interrumpir las operaciones o facilitar actividades
4. Integridad de la carga	Alteración, sabotaje o robo, o todas ellas, con fines terroristas.
5. Uso no autorizado	Realización de operaciones en la cadena de suministro internacional, para facilitar un incidente terrorista (incluido el uso del medio de transporte como arma).
6. Otros	

Durante la evaluación considere lo siguiente:

1) Control del acceso

- en las instalaciones de la organización en la cadena de suministro, incluido el vecindario;
- en los medios de transporte (camiones, ferrocarriles, aviones, barcazas, barcos, etc.);
- a la información;
- otros.

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

- operación normal;
- talleres de mantenimiento;
- cambios debidos a fallas;
- cambio de medios de transporte;
- Medios de transporte cuando están en reposo;
- uso de medios de transporte como arma;
- Otros.

3) Alteración

- Carga;
- Fabricación;
- Almacenamiento (incluido almacenamiento intermedio);
- Transferencia;
- Descarga;
- Desconsolidación / consolidación;
- Otros.

4) Transporte de mercancías por:

- aire;
- carretera;
- ferrocarril;
- despacho por corrientes de agua interiores;
- despacho por mar;
- otros.

5) Prevención / detección de la intromisión aplicada a los despachos

6) Durante las inspecciones, por ejemplo, las inspecciones de los vehículos

7) Empleados

- Nivel de competencia, entrenamiento y toma de conciencia;
- Integridad;
- otros.

8) Uso de socios comerciales

9) Comunicación interna/externa:

- Intercambio de información;
- situaciones de emergencia;
- Otros.

10) Manejo o procesamiento de información acerca de las rutas de carga o de transporte

- Protección de datos;
- Aseguramiento de datos;
- Otros.

11) Información externa

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

B.3 PASO DOS. CLASIFICACIÓN DE LAS CONSECUENCIAS

Una evaluación de las consecuencias debería considerar la pérdida potencial de vidas y las pérdidas económicas. Las consecuencias de cada incidente de seguridad evaluado en la cadena de suministro se debería clasificar como alto, medio o bajo (véase la Tabla 2). Se puede usar un sistema numérico en el proceso de evaluación, en tanto los resultados numéricos se conviertan a un sistema cualitativo.

Los fundamentos para la clasificación de las consecuencias para cada incidente de seguridad se deberían documentar.

Es conveniente tener cuidado al establecer valores de consecuencias "altas", "medias" y "bajas". El uso de valores umbral excesivamente bajos puede dar como resultado el requisito de que las contramedidas sean consideradas para más escenarios de amenazas a la seguridad de los necesarios. Sin embargo, el uso de valores umbral excesivamente altos puede omitir contramedidas para los escenarios de amenaza a la seguridad que involucran consecuencias que la organización o el gobierno dentro del que opera no pueden tolerar.

Una clasificación de consecuencia "alta" se puede considerar como una consecuencia que sería inaceptable en todas las situaciones, excepto en las de baja posibilidad.

Una clasificación de consecuencia "media" se puede considerar como una consecuencia que sería inaceptable en una situación de posibilidad alta.

Una clasificación de consecuencia "baja" se puede considerar como una consecuencia que es normalmente aceptable.

La aceptabilidad no se debería confundir con la conveniencia o aprobación. Más bien, la aceptabilidad se puede considerar como un juicio de la cantidad de daño posible que la organización o gobierno bajo el que opera está dispuesto a aceptar bajo algunas condiciones relacionadas con la probabilidad. Una organización o gobierno puede determinar que la posibilidad de algún nivel de daño puede ser indeseable aunque aceptable.

Asignar un Valor	Consecuencia
Alto	**Muerte y lesión.** Pérdida de la vida en una escala determinada. **o** **Impacto económico.** Daño considerable a un activo o infraestructura, o ambos, que impide operaciones posteriores. **o** **Impacto ambiental.** Destrucción completa de múltiples aspectos del ecosistema en un área extensa, **o todos los anteriores.**
Medio	**Muerte y lesión.** Por ejemplo, pérdida de la vida, **o** **Impacto económico.** Por ejemplo, daño a los activos o infraestructura, o ambos, que requiere reparaciones. **o** **Impacto ambiental.** Por ejemplo, daño a largo plazo a una porción del ecosistema, **o todos los anteriores.**
Bajo	**Muerte y lesión.** Lesiones, pero sin pérdida de la vida **o** **Impacto económico.** Daño mínimo a un activo o infraestructura, o a ambos, y a los sistemas. **o** **Impacto ambiental.** Algún daño ambiental **o todos los anteriores.**

B.4 PASO TRES. CLASIFICACIÓN DE LA POSIBILIDAD DE INCIDENTES DE SEGURIDAD

La categoría de las medidas de seguridad operativas y físicas en la cadena de suministro como están documentadas en la lista de revisión del desempeño y otra documentación suministrada, se deberían tener en cuenta al clasificar los incidentes de seguridad potenciales. Las medidas de seguridad físicas incluyen objetos que impiden o detectan el acceso no autorizado a una meta. Las medidas de seguridad operativas incluyen personas y procedimientos que impiden o detectan acceso no autorizado a una meta. La posibilidad de que cada incidente de segundad ocurra en un activo particular se debería clasificar como alto, medio y bajo.

- **Posibilidad alta** se debería usar cuando las medidas de seguridad implementadas ofrecen poca resistencia al incidente de seguridad que ocurre. Si se usa un sistema numérico en el proceso de evaluación, los resultados numéricos se deberían convertir a este sistema cualitativo.
- **Posibilidad media** se debería usar cuando las medidas de seguridad implementadas ofrecen resistencia moderada al incidente de seguridad que ocurre.

- **Posibilidad baja** se debería usar cuando las medidas de seguridad implementadas ofrecen resistencia considerable al incidente de seguridad que ocurre.

Se debería documentar el fundamento para la clasificación de la posibilidad asignada a cada incidente de seguridad.

B.5 PASO CUATRO. PUNTAJE PARA INCIDENTES DE SEGURIDAD

El gráfico de incidentes de seguridad presentado en la Tabla B.3 es un ejemplo que se puede usar para determinar cuándo se deberían usar contramedidas para incidentes de seguridad específicos.

Tabla B.3 Gráfico de puntajes para incidentes de seguridad

Clasificación de posibilidades Alta Media Baja				
Clasificación de consecuencias	Alta	Contramedidas	Contramedidas	Considerar
	Media	Contramedidas	Contramedidas o considerar, según sea apropiado	Documentar
	Baja	Considerar	Documentar	Documentar

La identificación de las contramedidas se requiere para incidentes de seguridad que tengan un puntaje alto tanto en posibilidad como en consecuencias, al igual que para los que alcanzan puntajes en posibilidad media y consecuencias altas. La persona que evalúa la seguridad debería hacer una lista de cada incidente de seguridad requerido para ser considerado para las contramedidas.

NOTA Los funcionarios gubernamentales y otros funcionarios que vigilan la aplicación de la ley pueden especificar contramedidas para algunos escenarios con consecuencias extremadamente altas, que van a ser promulgados como un asunto de política nacional, independientemente de su posibilidad. Las contramedidas desarrolladas como resultado de esta excepción deberían ser revisadas por el gobierno que requiere su eficacia.

B.6 PASO CINCO. DESARROLLO DE CONTRAMEDIDAS

Si el evaluador exige o considera recomendable el desarrollo de una contramedida, se deberían considerar las consecuencias o la posibilidad del escenario de amenazas a la seguridad, para su mitigación. La meta es la reducción de la posibilidad de que el escenario de amenazas a la seguridad tenga éxito, o la reducción del peligro que puede ser causado por los escenarios de amenaza a la seguridad a un nivel en el que ya no se requieran contramedidas adicionales.

Las contramedidas pueden ser algunas de las siguientes acciones:

- **Tratar:** pueden ser medidas organizacionales o físicas, o ambas.
- **Transferir:** la transferencia se puede hacer mediante subcontratación, transferencia física a otros lugares, tiempo, etc.
- **Terminar:** es posible que debido al nivel de riesgo la organización decida no continuar con las actividades.

En algunas circunstancias, una organización puede tener que tolerar (véase la nota) un riesgo debido a lo poco prácticas que son las contramedidas necesarias, a la falta de autoridad para imponer las medidas necesarias o a otros factores no superables.

NOTA Tolerar la situación implica que la organización no puede emprender ninguna acción. Estas actividades y evaluaciones se deberían documentar y revisar periódicamente.

B.7 PASO SEIS. IMPLEMENTACIÓN DE CONTRAMEDIDAS

Las nuevas contramedidas representan un cambio en las prácticas operativas y necesitan ser promulgadas de acuerdo con el sistema de gestión de la organización, para asegurar que los recursos adecuados están disponibles; se maneja el impacto sobre otras operaciones y el cambio cuenta con el soporte de la dirección.

B.8 PASO SIETE. EVALUACIÓN DE LAS CONTRAMEDIDAS

Usando los métodos especificados en esta norma, cada contramedida se debería evaluar en cuanto a su eficacia para reducir las posibilidades y las consecuencias (o una combinación de ellas) hasta que el riesgo para la seguridad no requiera que se consideren contramedidas adicionales. La contramedida que logre esto se considera eficaz y se debería incluir en el informe de evaluación de seguridad.

B.9 PASO OCHO. REPETICIÓN DEL PROCESO

Después de que se han desarrollado y evaluado contramedidas eficaces, se continúa el proceso para el siguiente escenario de evaluación de amenazas a la seguridad, hasta agotar la lista de escenarios.

B.10 CONTINUACIÓN DEL PROCESO

El proceso de evaluación es continuo. Como lo ilustra la Figura B.1, se debe hacer seguimiento continuo a la seguridad, para asegurar que las medidas de seguridad se lleven a cabo en la forma prevista, y que el proceso de evaluación se lleve a cabo de acuerdo con las necesidades.

ANEXO C
*(*Informativo*)*

GUÍA PARA OBTENER ASESORÍA Y CERTIFICACIÓN

C.1 GENERALIDADES

Las organizaciones que buscan implementar la norma ISO 28001 no están obligadas a utilizar los servicios de un consultor externo. Si una organización determina que necesita asesoría o ayuda para llevar a cabo evaluaciones de seguridad, desarrollar planes de seguridad o implementar los requisitos necesarios, puede buscar servicios de consulta externa. Sin embargo, es responsabilidad de la organización que busca la asesoría, revisar y verificar la competencia de los consultores que ofrecen estos servicios; por ejemplo, buscar recomendaciones, confirmar las referencias o revisar el trabajo realizado. Los consultores que brindan servicios a la organización estarían impedidos para participar en auditorías por tercera parte de la misma organización.

C.2 DEMOSTRACIÓN DE LA CONFORMIDAD CON LA NORMA ISO 28001 MEDIANTE AUDITORÍA

La norma ISO 28001 es una norma de requisitos prevista para ayudar a las organizaciones que optan voluntariamente por implementar los requisitos, a establecer y demostrar el nivel apropiado de seguridad dentro de las partes de la cadena de suministro internacional que controlan. Por tanto, sirve como base para determinar, validar o demostrar el nivel de seguridad existente dentro de la cadena de suministro de una organización por medio de un proceso de auditoría de primera, segunda o tercera parte, o por cualquier agencia gubernamental que elija usar la conformidad con esta norma como la base para la aceptación en sus programas de seguridad de la cadena de suministro.

Tipos de auditoría:

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

Validación y certificación por el gobierno o agencia gubernamental.

Las agencias gubernamentales que escogen usar la conformidad con esta norma como la base para aceptación en sus programas de seguridad de la cadena de suministro pueden certificar y validar ellos mismos esta conformidad o para evitar la duplicación pueden escoger contar con auditorías por otras partes. La OMA establece directrices para las administraciones de aduanas acerca de los requisitos de validación y certificación para los programas de seguridad de la cadena de suministro de aduanas nacional, de conformidad con el marco SAFE de la OMA y para el reconocimiento mutuo de estos programas.

C.3 CERTIFICACIÓN DE LA NORMA ISO 28001 POR ORGANISMOS DE CERTIFICACIÓN POR TERCERA PARTE

Si la demostración de conformidad se busca a través de un proceso de auditoría por tercera parte, entonces la organización que busca la certificación debería considerar seleccionar un organismo de certificación por tercera parte acreditado por un organismo de acreditación competente, tales como los miembros del Foro Internacional de Acreditación (IAF), y sujeto al Acuerdo de Reconocimiento Multilateral (MLA). Estos organismos de certificación acreditados cumplen los reglamentos, códigos de práctica y protocolos de auditoría reconocidos internacionalmente, tales como la norma ISO 17021 y la norma ISO 19011. Véase la sección sobre notas.

BIBLIOGRAFÍA

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

[2] ISO 14001:2004, Sistemas de Gestión Ambiental. Requisitos con orientación para su uso.

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

[4] ISO 17712:2006, Freight Containers. Mechanical Seáis

[5] ISO 19011:2002, Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiente.

[6] ISO/PAS 20858:2004, Ships and Marine Technology. Maritime Port Facility Securíty Assessments and Securíty Plan Development.

[7] ISO/PAS 28000:2007, Specification for Securíty Management Systems for the Supply Chain.

[8] ISO/PAS 28003:2007, Securíty Management Systems for the Supply Chain -Requirements for Bodies Providing Audit and Certification of Supply Chain Securíty Management Systems.

[9] International Safety Management (ISM) Code, International Maritime Organization

[10] SAFE Framework of Standards. Appendix to Annex 1, World Customs Organization.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZARON. *Security Management Systems for the Supply Chain. Best Practices for Implementing Supply Chain Security. Assessments and Plans. Requirements and Guidance.* Geneve, ISO 28001: 2007(E), p 27.

NORMA TÉCNICA COLOMBIANA NTC-ISO 28004

2009-02-18

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO. DIRECTRICES PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 28000

ICONTEC

E: SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN. GUIDELINES FOR THE IMPLEMENTATION OF ISO 28000.

CORRESPONDENCIA:
Esta norma es una adopción idéntica por traducción (IDT), respecto a su documento de referencia, la norma ISO 28004:2007.

DESCRIPTORES:
Logística; cadena; suministro; sistema

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

PROLOGO

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 28004 fue ratificada por el Consejo Directivo del 2009-02-18.

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.

ALPINA S.A.
AXÓNICA
CARROCERÍAS BENFOR
Cl. DISAN S.A.
COLFECAR
COLSEGUROS
COLTANQUES
INLAC
ICOLLANTAS
METROPYME
SOANSES LTDA-
SOCIEDAD TRACTEC
TITADSU
TRANSPORTE BOTERO SOTO

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

3M COLOMBIA
ABBOTT LABORATORES DE COLOMBIA S.A.
ACCIÓN SOCIAL - PRESIDENCIA DE LA REPÚBLICA
ACERÍAS DE CALDAS S.A.
ACERÍAS DE COLOMBIA -ACESCO-
ASOCIACIÓN COLOMBIANA DE LA MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS -ACOPI-
ACUAVIVA S.A E.S.P
ACUEDUCTO DE BOGOTÁ
ALCALDÍA MUNICIPAL DE CALI
ALDÍA LOGÍSTICA
ALFA SERVICIOS DE GESTIÓN EMPRESARIAL
ALIMENTOS KRAFT
ALKOSTO
ALMACENAR
ALMACENES ÉXITO
ALMACENES GENERALES DE DEPÓSITO GRAN COLOMBIA S.A. -ALMAGRAN-
ALPINAS.A.
ALTHVIZ & CÍA. LTDA.
ANALDEX
ASOCIACIÓN NACIONAL DE INDUSTRIALES -ANDI-

ASOCIACIÓN DE TRANSPORTADORES INDEPENDIENTES -ATRIN-
ASOCIADOS DISTRIBUIDORES DE DERIVADOS DEL PETRÓLEO -ADISPETROL-
ASOCIACIÓN COLOMBIANA DEL PESAJE -ASOPESAJE-
ASOCIACIÓN NACIONAL DE TRANSPORTADORES -ASOTRANS-
ASESORÍAS TÉCNICAS CORREDORES DE SEGUROS -ASTEC-
ATENCIÓN TÉCNICA EN CALIDAD LTDA.
AUTO AIRES S.A.
AUTO FUSA S.A.
AVON
BAVARIA S.A.
BEC INTERNATIONAL LTDA.
BUREAU VERITAS CERTIFICARON
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. GARULLA
CARVAJAL S.A.
CASA LUKER S.A.
CENTELSA
CENTRALES DE TRANSPORTES S.A.
CENTRORIENTE S.A.
CHALLENGER S.A.
CHALLENGER
CÍA COLOMBIANA DE TRANSPORTES S.A. -COLDETRANS S.A.-
CLÍNICA DE OCCIDENTE S.A.
COCA-COLA - PANAMCO COLOMBIA S.A.
COLCERÁMICA
COLGATE PALMOLIVE
COLOMBIANA DE TANQUES LTDA. -COLTANQUES LTDA.-
COLOMBIANA KIMBERLY COLPAPEL S.A.
COMFAMA
COMFENALCO SANTANDER
COMPAÑÍA COLOMBIANA AUTOMOTRIZ
COMPAÑÍA DE CARGA MOVITRANSPORTES LTDA.
COMPAÑÍA DE DISTRIBUCCIÓN 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.
INCELTS.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
LUMINEXS.A.
MARQUES Y URIZA LTDA
MICHELIN COLOMBIA
MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
MINISTERIO DE TRANSPORTE
MOTORIZADOS EXPRESS LTDA.
MOTOTRANSPORTAR S.A.
MOVÍ STAR
MULTINACIONAL TRANSPORTADORA LTDA
MUNDIAL DE ALUMINIOS
MURALLA SEGURIDAD LTDA.
NESTLÉ 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 SA-
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.
SECRETARÍA 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.
TECNOQUIMICAS 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 & CÍA. LTDA
TRANSPORTES MULTIGRANEL S.A.
TRANSPORTES PREMMIER LTDA.
TRANSPORTES SIVAL
TRANSPORTES TERRESTRES DE CARGA LTDA.
TRANSPORTES VIGÍA 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.

DIRECCIÓN DE NORMALIZACIÓN

INTRODUCCIÓN

La norma ISO 28000:2007, Sistemas de gestión de la seguridad para la cadena de suministro, y esta norma se han desarrollado como respuesta a la necesidad de una norma reconocible de un sistema de gestión para la cadena de suministro frente a la cual puedan evaluarse y certificarse sus sistemas de gestión de la seguridad y de una guía para la implementación de una norma de esa clase.

La norma ISO 28000 es compatible con las normas de sistemas de gestión ISO 9001:2002 (calidad) e ISO 14001:2004 (ambiental). Estas facilitan la integración de los sistemas de gestión de la cadena de suministro, de calidad y ambiental de las organizaciones, siempre y cuando que estas quieran hacerlo.

Esta norma incluye un recuadro al comienzo de cada numeral/subnumeral, que presenta los requisitos completos a partir de la norma ISO 28000 y está seguida por la guía pertinente. La numeración de los numerales de esta norma corresponde con la de la norma ISO 28000.

Esta norma se revisará o se ajustará cuando se considere apropiado hacerlo. Se procederá a hacer ajustes se revise la norma ISO 28000.

Esta norma no pretende incluir todas las disposiciones necesarias de un contrato entre los operadores de la cadena de suministro, los proveedores y las partes interesadas. Los usuarios son responsables de su correcta aplicación.

El cumplimiento de esta norma no confiere, por sí sola, inmunidad en cuanto a obligaciones legales.

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO. DIRECTRICES PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 28000

1. OBJETO Y CAMPO DE *APLICACIÓN*

Esta norma proporciona una recomendación genérica sobre la implementación de la norma ISO 28000:2007, Sistemas de gestión de la seguridad para la cadena de suministro.

Explica los principios subyacentes de la norma ISO 28000 y describe el propósito, las entradas típicas, los procesos y resultados típicos, para cada requerimiento de la norma ISO 28000. Esto con el fin de ayudar a la comprensión e implementación de la norma ISO 28000.

Esta norma no crea requisitos adicionales a los especificados en la norma ISO 28000, ni ordena enfoques obligatorios para la implementación de la norma ISO 28000.

ISO 28000

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma específica 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 por 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 la norma ISO 28000.

3. TÉRMINOS Y DEFINICIONES

ISO 28000

3. TÉRMINOS Y DEFINICIONES

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.

Para los propósitos del presente documento, los términos y definiciones dados en la norma ISO 28000 y siguientes tienen implementación.

3.1 Riesgo. Probabilidad de materialización de una amenaza a la seguridad y sus consecuencias.

3.2 Certeza de seguridad. Proceso de verificar la fidelidad de las personas que tendrán acceso a material sensible sobre seguridad.

3.3 Amenaza. Cualquier posible acción o serie de acciones intencionales con daño potencial a cualquiera de los partes interesadas, a las instalaciones, al funcionamiento, a la cadena de suministro, a la sociedad, a la economía o a la continuidad e integridad del negocio.

4. ELEMENTOS DEL SISTEMA GESTIÓN DE LA SEGURIDAD

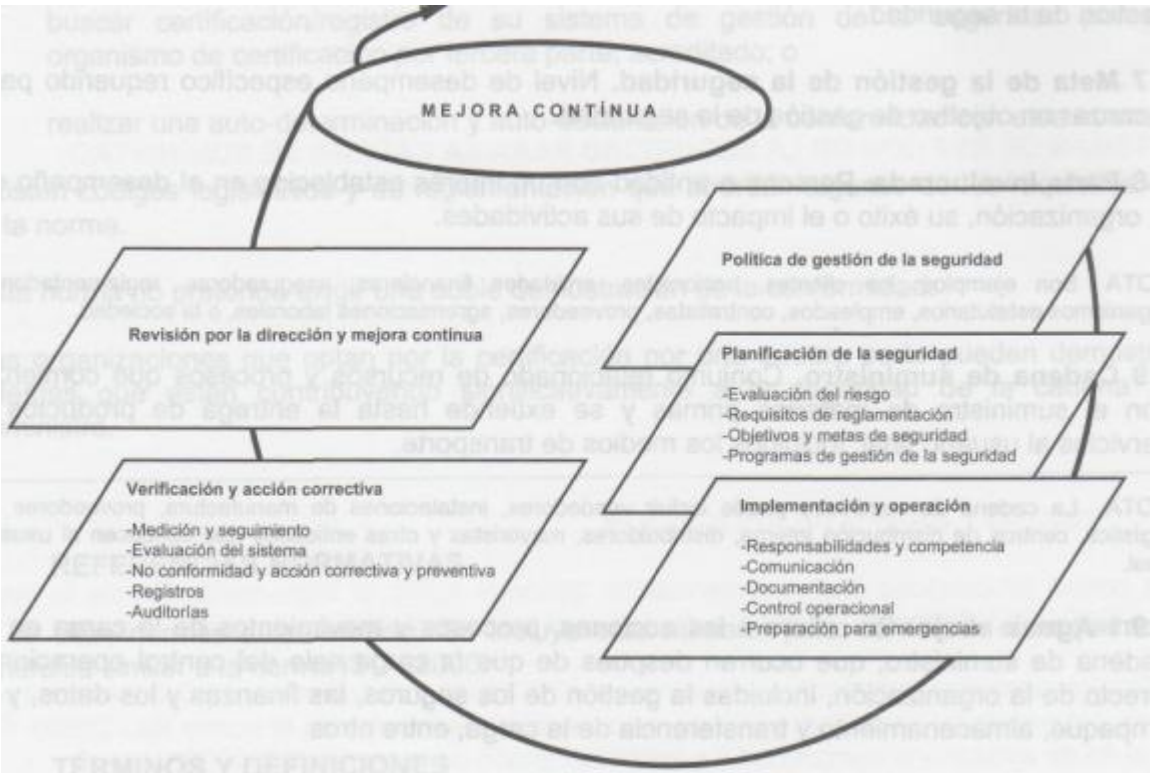

Figura 1. Elementos del sistema de gestión de la seguridad

4.1 REQUISITOS GENERALES

a) Requisito de la norma ISO 28000

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.

b) Propósito

La organización debería establecer y mantener un sistema de gestión que sea conforme con todos los requisitos de la norma ISO 28000. Esto puede ayudar a la organización a cumplir con las regulaciones, requisitos y leyes sobre seguridad.

El nivel de detalle y complejidad del sistema de gestión de la seguridad, la cantidad de documentación y los recursos dedicados a él depende del tamaño y complejidad de una organización y la naturaleza de sus actividades.

Una organización tiene la libertad y flexibilidad para definir sus límites y puede escoger implementar la norma ISO 28000 con respecto a toda la organización o a determinadas operaciones especificas o actividades de la organización.

Debería tenerse cuidado al definir los límites y alcance del sistema de gestión. Las organizaciones no deberían tratar de limitar su alcance de modo que excluya de la evaluación una operación o actividad que se requiera para el funcionamiento general de la organización o aquellos que puedan incidir en la seguridad de sus empleados y otras partes interesadas.

Si se implementa la norma ISO 28000 para una operación especifica o actividad, las políticas y procedimientos de seguridad desarrollados por las demás partes de la organización puede tener capacidad de utilizarse por esa operación especifica o actividad para ayudar a reunir los requisitos de la norma ISO 28000. Esto puede requerir que esas políticas o procedimientos de seguridad se sometan a una pequeña revisión o enmienda, para asegurarse de que ellos son aplicables a dicha operación especifica o actividad.

c) Entradas típicas

Todos los requisitos de entrada se especifican en la norma ISO 28000.

d) Resultado típico

Un resultado típico es un sistema de gestión de la seguridad implementado y mantenido eficazmente que ayuda a la organización en la búsqueda de mejora continua.

4.2 POLÍTICA DE GESTIÓN DE LA SEGURIDAD

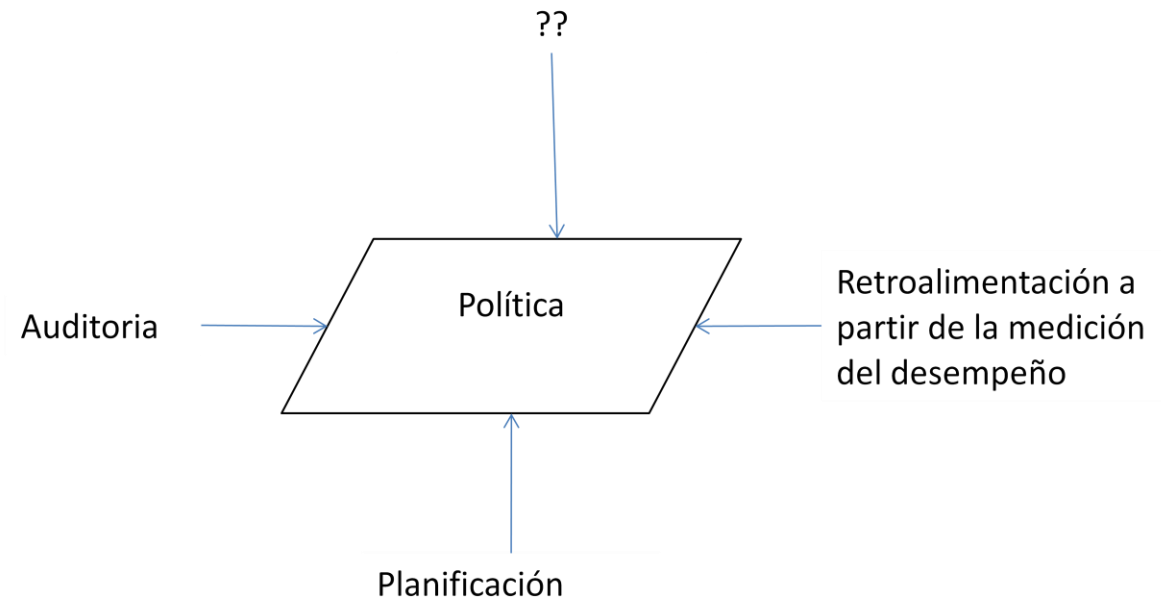

Figura 2. Política de gestión de la Seguridad

a) Requisito de la norma ISO 28000

La alta dirección de la organización debe autorizar una política de gestión de la segundad 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 segundad;

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.

b) Propósito

Una política de seguridad es una declaración concisa del compromiso de la alta gerencia respecto a la seguridad. Una política de seguridad establece un sentido

general de dirección y fija los principios de acción para una organización. Fija los objetivos de seguridad para la responsabilidad y desempeño sobre seguridad que requieren a lo largo de la organización.

La alta gerencia de la organización debería producir y autorizar una política de seguridad documentada.

c) Entradas típicas

Al establecer la política de seguridad, la dirección debería considerar los siguientes factores, sobre todo en cuanto a su cadena de suministro:

- política y objetivos pertinentes al negocio de la organización como un todo;
- desempeño de seguridad tanto histórico como actual de la organización;
- necesidades de las partes interesadas;
- oportunidades y necesidades para la mejora continua;
- recursos necesarios;
- contribución de los empleados;
- contribución de los contratistas, partes interesadas y otro personal externo.

d) Proceso

Cuando establece y autoriza una política de seguridad, la alta gerencia debería tener en cuenta los puntos que se indican a continuación.

Una política de seguridad formulada y comunicada eficazmente debería:

1) Ser apropiada a la naturaleza y escala de los riesgos de seguridad de la organización;

La identificación de amenazas, la evaluación del riesgo y la gestión del riesgo están en el núcleo de un exitoso sistema de gestión de la seguridad y deberían reflejarse en la política de seguridad de la organización.

La política de seguridad debería ser consistente con una visión del futuro de la organización. Debería ser realista y no debería exagerar la naturaleza de los riesgos que la organización enfrenta, ni subestimarlos.

2) Incluir un compromiso con la mejora continua;

Las amenazas globales a la seguridad aumentan la presión en las organizaciones para reducir el riesgo de incidentes en la cadena de suministro. Además de cumplir con las responsabilidades legales, nacionales y de regulación, así como otras regulaciones y pautas preparadas por las organizaciones como la Organización Aduanera Mundial (WCO), la organización debería apuntar a mejorar su desempeño de seguridad y su sistema de gestión de la seguridad, efectiva y eficazmente, para satisfacer las necesidades de cambio del comercio global, las del negocio y las necesidades regulatorias.

El mejoramiento del desempeño planeado debería expresarse en los objetivos de seguridad (véase el numeral 4.3.2) y manejarse a través del programa de gestión de la seguridad (véase el numeral 4.3.5) aunque la declaración de política de seguridad puede incluir amplias áreas de acción.

3) Incluir un compromiso para al menos dar conformidad a las actuales regulaciones de seguridad aplicables y con otros requisitos a los cuales se subscribe la organización

Se exige a las organizaciones acomodarse a los requisitos regulatorios de seguridad aplicables. El compromiso de la política de seguridad es un reconocimiento público de la organización acerca de que tiene un deber al cual acatar, si no excede, ninguna legislación, u otros requisitos, obligatorios por la ley o adoptados voluntariamente a los cuales está suscrita, como el marco de normas WCO SAFE.

NOTA La expresión "Otros requisitos" puede significar, por ejemplo, políticas corporativas o de grupo, las propias normas internas de la organización o las especificaciones o códigos de práctica a los que se subscribe la organización.

4) Documentarse, implementarse y mantenerse.

La planificación y la preparación son la clave para la implementación exitosa. A menudo las declaraciones de la política de seguridad y los objetivos de seguridad son poco realistas porque hay inadecuados o inapropiados recursos disponibles para entregar. Antes de hacer cualquier declaración pública la organización debería asegurarse de que toda financiación, habilidades y recursos necesarios están disponibles y de que todos los objetivos de seguridad son realmente alcanzables dentro de este marco.

Para que la política de seguridad sea eficaz, debería documentarse y debería revisarse periódicamente para continuar la adecuación y debería ajustarse o revisarse si fuese necesario.

5) Comunicarse a todos los empleados, con el supuesto de que los empleados son conscientes de sus obligaciones de seguridad individuales

La participación y el compromiso de los empleados son vitales para la seguridad exitosa.

Los empleados necesitan hacerse conscientes de los efectos de la gestión de la seguridad sobre la calidad de su propio ambiente de trabajo y deberían estimularse a contribuir activamente en la gestión de la seguridad.

Los empleados (a todos los niveles, incluso los niveles de gerencia) probablemente no sean capaces de hacer una contribución eficaz a la gestión de la seguridad, a menos que entiendan la política de la organización y sus responsabilidades y sean competentes para desempeñar sus tareas requeridas.

Esto exige que la organización comunique sus políticas de seguridad y objetivos de seguridad claramente a sus empleados, para permitirles tener un marco frente al cual pueden medir su propio desempeño de seguridad individual.

6) Estar disponible a los partes interesadas

Cualquier individuo o grupo (interno o externo) interesado en el desempeño de seguridad de la organización o afectado por éste estaría particularmente interesado en la declaración de política de seguridad. Por consiguiente, debería existir un proceso para comunicarles a ellos la política de segundad. El proceso debería asegurar que las partes interesadas reciban la política de seguridad donde corresponda.

7) Ser revisado periódicamente para asegurarse de que mantiene su pertinencia y apropiación para la organización

El cambio es inevitable, las regulaciones y la legislación evolucionan y las expectativas de las partes interesadas aumentan. En consecuencia, la política de seguridad y el sistema de gestión de la organización debería revisarse regularmente para asegurar su continua conveniencia y efectividad.

Si se introducen cambios, estos deberían comunicarse en cuanto sea factible hacerlo.

e) Resultado típico

Un resultado típico es una política de seguridad comprensiva, concisa y comprensible a lo largo de la organización y para las partes interesadas según sea necesario.

4.3 EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PLANIFICACIÓN

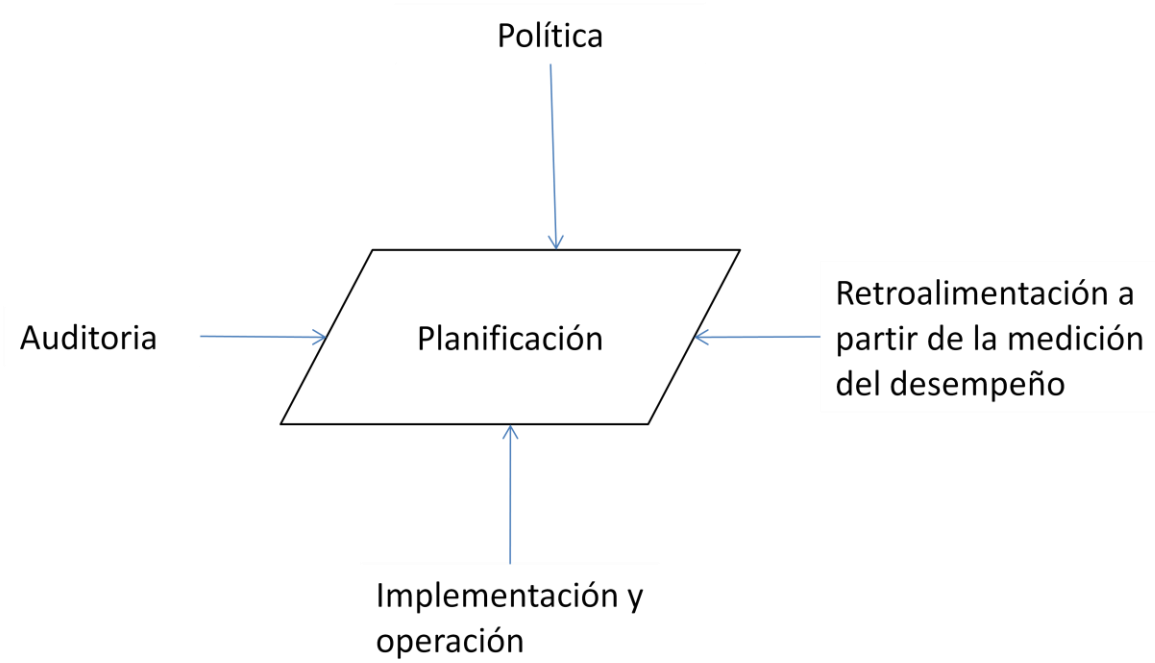

Figura 3. Plano

4.3.1 Evaluación del riesgo de seguridad

a) Requisito de la norma ISO 28000

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).

b) Propósito

La organización debería tener una apreciación total del riesgo de seguridad significativo, de las *amenazas y* vulnerabilidades que éste *abarca,* después de utilizar los procesos de identificación de amenazas a la seguridad, evaluación del riesgo y gestión del riesgo.

La identificación de amenaza a la segundad, los procesos de evaluación del riesgo y gestión del riesgo y sus resultados deberían ser la base de todo el sistema de seguridad. Es importante que los nexos entre los procesos de identificación de amenaza a la seguridad, la evaluación del riesgo y la gestión del riesgo y los demás elementos del sistema de gestión de la seguridad estén claramente establecidos y visibles.

El propósito de esta pauta es establecer principios por los cuales la organización pueda determinar, dada la identificación de amenaza a la seguridad, si los procesos de evaluación del riesgo y de gestión del riesgo son o no convenientes y suficientes. El propósito no es hacer recomendaciones sobre la manera como deberían dirigirse estas actividades.

Los procesos de identificación de la amenaza a la segundad, evaluación del riesgo y gestión del riesgo deberían permitir a la organización identificar, evaluar y controlar sus riesgos de seguridad sobre una base de continuidad.

En todos los casos, debería darse consideración a las operaciones normales y anormales dentro de la organización y a las potenciales condiciones de emergencia.

La complejidad de los procesos de identificación de la amenaza a la seguridad, evaluación del riesgo y gestión del riesgo depende considerablemente de factores como el tamaño de la organización, las situaciones de lugar de trabajo dentro de la organización y la naturaleza, complejidad e importancia del riesgo de seguridad. No es propósito de la norma ISO 28000:2007 (véase el numeral 4.3.1) forzar a las pequeñas organizaciones que tienen un riesgo de seguridad muy limitado a emprender complejos ejercicios de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo.

Los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo deberían tener en cuenta el costo y el tiempo necesarios para realizar

estos tres procesos y la disponibilidad de datos fiables. En estos procesos puede usarse información ya desarrollada para propósitos regulatorios u otros. La organización también puede tener en cuenta el grado de control práctico que puede tener sobre las amenazas a la seguridad que están en consideración. La organización debería determinar cuáles son sus amenazas a la seguridad, teniendo en cuenta las entradas y los resultados que están asociados a sus actuales y pasadas actividades, procesos, productos y/o servicios pertinentes.

La evaluación del riesgo de seguridad debería ser dirigida por personal calificado utilizando metodologías reconocidas que puedan documentarse.

Una organización en la que no exista un sistema de gestión de la seguridad puede establecer su posición actual con respecto a los riesgos a la segundad por medio de una evaluación del riesgo. El objetivo debería ser el de considerar las amenazas a la seguridad afrontadas por la organización, como base para establecer el sistema de gestión de la seguridad. Una organización debería considerar la inclusión de los siguientes factores dentro de su revisión inicial, aunque sin limitarse a ellos:

- requisitos legislativos y de regulación;
- identificación de las amenazas a la seguridad afrontadas por la organización;
- búsqueda de la amenaza a la seguridad y la información sobre riesgo a partir de las apropiadas organizaciones policiales y de inteligencia;
- un examen de todas las prácticas, procesos y procedimientos de gestión de la seguridad existentes;
- una evaluación de retroalimentación a partir de la investigación de incidentes y emergencias previos.

Una adecuada aproximación a la evaluación puede incluir listas de verificación, entrevistas, inspección y medición directas, resultados de previas auditorías del sistema de gestión u otras revisiones que dependen de la naturaleza de las actividades. Todas estas tareas deberían seguir una metodología replicable que esté documentada.

Conviene hacer énfasis en que se recomienda una revisión inicial para crear una línea de base pero no es un sustituto para la implementación de! enfoque sistemático estructurado que se indica en la parte restante del numeral 4.3.1.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- aspectos legales y otros requisitos de seguridad (véase el numeral 4.3.2);
- política de seguridad (véase el numeral 4.2);
- registros de los incidentes:
- no conformidades (véase el numeral 4.5.3);
- resultados de la auditoría al sistema de gestión de la seguridad (véase el numeral 4.5.5);

- comunicaciones provenientes de los empleados y otras partes interesadas (véase el numeral 4.4.3);
- información proveniente de consultas de seguridad de los empleados, actividades de revisión y mejoramiento del lugar de trabajo (estas actividades pueden ser de naturaleza reactiva o proactiva);
- información sobre las mejores prácticas, el riesgo típico de seguridad respecto de la organización, los incidentes y emergencias que hayan ocurrido en organizaciones similares;
- normas de la industria; advertencias gubernamentales;
- información sobre las instalaciones, procesos y actividades de la organización, incluyendo lo siguiente:
    - detalles de los cambios de procedimientos de control;
    - plan (planes) de locación
    - manuales sobre procesos y procedimientos operacionales;
    - datos de seguridad;
    - datos de seguimiento (véase el numeral 4.5.1).

d) Proceso

1) Identificación de la amenaza a la seguridad, evaluación del riesgo y gestión del riesgo

i) General

Las medidas para la gestión del riesgo deberían reflejar el principio de eliminación o reducción de un riesgo de seguridad mínimo factible, donde corresponda, ya sea reduciendo la probabilidad de ocurrencia o la severidad potencial de los impactos a partir de los incidentes de seguridad relatados. Los procesos de identificación de amenaza a la segundad, evaluación del riesgo y gestión del riesgo son herramientas clave en la gestión del riesgo.

Los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo varían considerablemente a través de las industrias, y van desde las simples evaluaciones hasta los complejos análisis cuantitativos con extensa documentación. Para que la organización planifique e implemente los apropiados procesos de identificación de amenaza a la seguridad, evaluación del riesgo y de gestión del riesgo, ésta satisface sus necesidades y sus situaciones acerca del lugar de trabajo y ayuda a que haya conformidad con cualquier requisito legislativo de seguridad.

Los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo deberían llevarse a cabo como medidas proactivas, más que como reactivas, es decir, deberían preceder a la introducción de nuevas o revisadas actividades o procedimientos. Cualquier medida necesaria que se identifique sobre control y reducción de riesgo debería implementarse antes de introducir los cambios.

La organización debería mantener su metodología, calificaciones personales, documentación, datos y registros que conciernen a la identificación de la amenaza, la evaluación del riesgo y gestión del riesgo actualizados respecto de las actividades que estén en marcha y también debería extenderlos para considerar nuevos desarrollos y nuevas o modificadas actividades, antes ponerlos en ejecución.

Los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo no sólo deberían aplicarse a las operaciones "normales" del medio y los procedimientos, sino también a las operaciones y procedimientos periódicos u ocasionales.

Al igual que considerar el riesgo de seguridad y los riesgos que surgen de las actividades llevadas a cabo por su propio personal, la organización debería considerar el riesgo de seguridad y los riesgos que surgen de las actividades de los contratistas y visitantes y del uso de productos o servicios proporcionados por otros a ella.

i i) Procesos

Los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo deberían documentarse y deberían incluir los siguientes elementos:

- identificación de amenazas a la seguridad;
- evaluación del riesgos con medidas del control existentes (o propuestas) en el lugar (tomando en cuenta la exposición a amenazas a la seguridad específicas, la probabilidad de falla de las medidas de control y la severidad potencial de las consecuencias de lesión, daño y continuidad operacional);
- evaluar la tolerabilidad del riesgo corriente y residual;
- identificación de cualquier medida adicional de gestión del riesgo que fuese necesaria;
- evaluación acerca de si las medidas de gestión del riesgo son suficientes para reducir el riesgo a un nivel tolerable.

Adicionalmente, los procesos deberían dirigirse a lo siguiente:

- la naturaleza, tiempos, alcance y metodología para cualquier forma de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo que vaya a usarse;
- legislación de seguridad aplicable u otros requisitos;

- los roles y autoridad del personal responsable de la realización de los procesos;
- los requisitos de competencia y las necesidades de entrenamiento (véase el numeral 4.4.2) para el personal que va a realizar los procesos. (Dependiendo de la naturaleza o del tipo de procesos que vaya a usarse, puede ser necesario que la organización recurra a asesoría o servicios externos);
- el uso de información proveniente de los entradas sobre seguridad de los empleados, las actividades de revisión y mejoramiento (estas actividades pueden ser de naturaleza reactiva o proactiva).

iii) Acciones subsiguientes

Siguiendo el desempeño de los procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo:

- debería haber clara evidencia de que cualquier acción correctiva o preventiva (véase el numeral 4.5.2) identificada como necesaria sea monitoreada en cuanto a su oportuna realización (esto puede requerir que se efectúen posteriores evaluaciones de identificación de amenaza a la seguridad y de riesgo, a fin de reflejar los cambios propuestos para las mediciones de gestión del riesgo y para determinar las estimaciones revisadas de los riesgos residuales);
- debería proporcionarse a la dirección una retroalimentación sobre los resultados y sobre el progreso de la realización de las acciones correctivas o preventivas, como entrada para la revisión por la dirección (véase el numeral 4.6) y para el establecimiento de objetivos de seguridad revisados o nuevos;
- la organización debería estar en posición de determinar si la competencia del personal que realiza determinadas tareas de seguridad es consistente con las especificadas por el proceso de evaluación del riesgo al establecer la necesaria gestión del riesgo;
- la retroalimentación proveniente de la subsiguiente experiencia de operación debería usarse para enmendar los procesos o los datos sobre los que se basa, en cuanto sea aplicable.

2) Después de la evaluación inicial de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo (véase también el numeral 4.6)

El proceso de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo debería revisarse en un momento o período predeterminado según se haya establecido en el documento de la política de seguridad, o en un momento predeterminado por la dirección, que puede formar parte del proceso de revisión por la dirección (véase el numeral 4.6). Este período puede variar, dependiendo de las siguientes consideraciones:

- la naturaleza de las amenazas a la seguridad;

- la magnitud del riesgo;
- cambios del funcionamiento normal.

La revisión también debería tener lugar si los cambios dentro de la organización ponen en cuestionamiento la validez de las evaluaciones existentes. Estos cambios pueden incluir los siguientes elementos:

- la expansión, reducción, reestructuración, cambios en los medios o aspectos de la cadena de suministro;
- la reasignación de responsabilidades;
- cambios en los métodos de trabajo o patrones de comportamiento de las amenazas a la seguridad provenientes de fuentes externas.

e) Resultados típicos

- Debería haber procedimientos documentados para los siguientes elementos:

  identificación de amenazas a la seguridad;
  - determinación de los riesgos asociados a las amenazas a la seguridad identificadas;
  - indicación del nivel de los riesgos relacionados con cada amenaza a la seguridad y si ellos son o tolerables o no;
  - descripción de o referencia a las medidas para seguimiento y controlar los riesgos (véanse los numerales 4,4.6 y 4.5.1), particularmente los riesgos que no son tolerables;
  - donde sea apropiado, los objetivos y acciones de seguridad para reducir los riesgos identificados (véase el numeral 4.3.3) y cualquier actividad de seguimiento para seguimiento el avance en su reducción;
  - identificación de la competencia y los requisitos de entrenamiento para implementar medidas de control (véase el numeral 4.4.2);
  - medidas de control necesarias detalladas como parte del elemento de control operacional del sistema (véase el numeral 4.4.6);
  - registros generados por cada uno de los procedimientos antes mencionados.

4.3.2 Requisitos de seguridad legales, estatutarios y otros regulatorios a)

Requisito ISO 28000

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.

b) Propósito

La organización debería ser consciente de y entender cómo sus actividades son o serán afectadas por los requisitos legales y otros que son aplicables y comunicar esta información al personal pertinente.

Este requisito de el numeral 4.3.2 proveniente de la norma ISO 28000:2007 tiene el propósito de promover el conocimiento y la comprensión de las responsabilidades legales y regulatorias. No pretende exigir a la organización establecer bibliotecas de documentos legales u otros que rara vez se referencian o se usan.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- detalles de la cadena de suministro de la organización;
- resultados de la identificación de amenaza a la seguridad, la evaluación del riesgo y la gestión del riesgo (véase el numeral 4.3.1);
- las mejores prácticas (por ejemplo, códigos, recomendaciones de asociaciones de la industria);
- requisitos legales, gubernamentales, intergubernamentales, las asociaciones de comercio, los códigos, prácticas y regulaciones;
- listado de fuentes de información;
- normas nacionales, regionales o internacionales;
- requisitos internos de la organización;
- requisitos de las partes interesadas;
- procesos para manejar la dinámica de la cadena de suministro.

d) Proceso

Deberían identificarse la legislación pertinente y otros requisitos. Las organizaciones deberían identificar los medios más apropiados para acceder a la información, incluyendo los medios que dan soporte a la información (por ejemplo, papel, CD, disco, Internet). La organización debería también evaluar qué requisitos tienen aplicación y dónde la tienen, y quién necesita recibir la información.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimientos para identificar la información y acceder a ella y mantenerla actualizada;
- identificación de cuáles requisitos tienen aplicación y dónde [esto puede tomar la forma de registro(s)];
- requisitos (el texto real, resumen o análisis, donde corresponda), disponibles en situaciones que serán decididas por la organización;
- procedimientos para seguimiento de la implementación de controles adecuados a la nueva legislación de seguridad.

4.3.3 Objetivos de la gestión de la seguridad

a) Requisito ISO 28000

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.

b) Propósito

Es necesario asegurarse de que, a lo largo de la organización (donde sea práctico hacerlo), se establezcan objetivos de seguridad medibles que sean consistentes con la política de segundad.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- política y objetivos pertinentes al negocio de la organización en su conjunto;
- política de seguridad, incluyendo el compromiso con la mejora continua (véase el numeral 4.2);
- resultados de la identificación de *amenaza a* la seguridad, evaluación del riesgo y gestión del riesgo (véase el numeral 4.3.1);
- requisitos legales y otros (véase el numeral 4.3.2);
- opciones tecnológicas;
- requisitos financieros, operacionales y comerciales;
- intereses de los empleados y las partes interesadas (véase el numeral 4.4.3);
- información proveniente de las entradas de seguridad, evaluaciones y actividades de mejoramiento en el lugar de trabajo de los empleados (estas actividades pueden ser de naturaleza reactiva o proactiva);
- análisis de los objetivos de seguridad establecidos;
- registros pasados de no conformidades de seguridad, incidentes y daño de propiedad;
- resultados de la revisión por la dirección (véase el numeral 4.6).

d) Proceso

Usando información o datos de las entradas, los niveles apropiados de la organización deberían identificar, establecer y priorizar los objetivos de seguridad.

Durante el establecimiento de los objetivos de seguridad, debería darse particular consideración a información o datos de aquellos que tienen más probabilidad de ser afectados por los objetivos de seguridad individuales, en la medida en que esto pueda ayudar a asegurar que ellos son razonable y ampliamente aceptados. También es útil considerar información o datos provenientes de fuentes externas a la organización; por ejemplo, de contratistas, proveedores, socios comerciales, policía y agencias de inteligencia o partes interesadas.

Los niveles de dirección apropiados deberían mantener reuniones regularmente para el establecimiento de objetivos de seguridad (por ejemplo, al menos con una frecuencia anual). Para algunas organizaciones puede haber necesidad de documentar el proceso de establecimiento de los objetivos de seguridad.

Los objetivos de seguridad deberían apuntar tanto a amplios elementos de seguridad corporativa como a elementos de seguridad que son específicos para suplir las cadenas, las funciones individuales y los niveles dentro de la organización.

Deberían definirse los indicadores adecuados para cada objetivo de seguridad, donde corresponda hacerlo. Estos indicadores deberían permitir el seguimiento de la implementación de los objetivos de seguridad.

Los objetivos de seguridad deberían ser razonables y alcanzables, en tanto que la organización debería tener la capacidad de alcanzarlos y monitorear el progreso. Debería definirse una escala de tiempo razonable y alcanzable para la realización de cada objetivo de seguridad.

Los objetivos de seguridad pueden descomponerse en metas separadas, dependiendo del tamaño de la organización, la complejidad del objetivo de seguridad y su periodo de tiempo. Debería haber claros nexos entre los diversos niveles de metas y objetivos de seguridad.

Ejemplos de tipos de objetivos de seguridad

son:

- la reducción de los niveles de riesgo;
- la introducción de rasgos adicionales en el sistema de gestión de seguridad;
- los pasos dados para mejorar los medios existentes;
- la eliminación o la reducción de la frecuencia de incidentes indeseados particulares.

Los objetivos de seguridad deberían comunicarse (por ejemplo, vía sesiones de entrenamiento o de grupos de información; véase el numeral 4.4.2) al personal pertinente y deberían desplegarse a través de los programas de gestión de segundad (véase el numeral 4.3.4).

e) Resultados típicos

Los resultados típicos incluyen objetivos de seguridad documentados, medibles donde sea factible, para cada función en la organización.

4.3.4 Metas de gestión de la seguridad

a) Requisito ISO 28000

La organización debe establecer, implementar y mantener las metas del sistema 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 las metas de gestión de la seguridad. Donde sea necesario los objetivos se deben ajustar consecuentemente.

b) Propósito

Las metas de seguridad se disponen para lograr el objetivo dentro del marco de tiempo especificado.

c) Entradas típicas

- política y objetivos pertinentes al negocio de las organizaciones como un todo;
- política de seguridad, incluyendo el compromiso hacia la mejora continua (véase el numeral 4.2);
- resultados de la identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo (véase el numeral 4.3.1);
- requisitos legales y otros (véase el numeral 4.3.2);
- opciones tecnológicas;
- requisitos financieros, operacionales y comerciales;
- intereses de los empleados y las partes interesadas (véase el numeral 4.4.3);
- información proveniente de las entradas de seguridad de los empleados, actividades de evaluación y de mejoramiento en el lugar de trabajo (estas actividades pueden ser de naturaleza reactiva o proactiva);
- análisis de los objetivos de seguridad establecidos;
- registros pasados de no conformidades de seguridad e incidentes;
- resultados de la revisión por la dirección (véase el numeral 4.6).

d) Proceso

El proceso se define en los programas de seguridad y consiste en las metas alcanzables para lograr el (los) objetivo(s).

Utilizando información o datos provenientes de las entradas, la gestión adecuada debería identificar, establecer y priorizar las metas de seguridad. Las metas deberían ser específicas, medibles y basados en cronogramas.

Durante el establecimiento de las metas de seguridad, debería darse especial atención a la información o los datos provenientes de aquellos que tienen más probabilidad de ser afectados por las metas de seguridad individuales, por cuanto esto puede ayudar a asegurase que los objetivos son razonables y ampliamente aceptados. También es útil considerar la información o los datos de fuentes externas a la organización; por ejemplo, contratistas, proveedores, socios comerciales, policía y agencias de inteligencia y partes interesadas.

Las reuniones de los niveles apropiados de la organización para establecer las metas de seguridad deberían revisar los objetivos de segundad después de ser modificados. Para algunas organizaciones puede ser necesario documentar el proceso de establecer las metas de seguridad.

Las metas de seguridad deberían apuntar tanto a los amplios aspectos de la seguridad corporativa como a los aspectos de seguridad que son específicos para la cadena de suministro, las funciones individuales y los niveles dentro de la organización.

Deberían definirse los indicadores adecuados para cada meta de seguridad. Estos indicadores deberían permitir el seguimiento de la implementación de las metas de seguridad.

Las metas de seguridad deberían ser razonables y alcanzables, y en ello, la organización debería tener la capacidad para alcanzarlas y hacer seguimiento del avance. Debería definirse un periodo de tiempo razonable y alcanzable para la realización de cada meta de seguridad.

Las metas de seguridad pueden descomponerse en metas separadas, dependiendo del tamaño de la organización, la complejidad de las metas de seguridad y su escala de tiempo. Debería haber vínculos claros entre los diversos niveles de metas y objetivos de seguridad.

Ejemplos de tipos de metas de seguridad son:

- reducción de los niveles de riesgo en un determinado periodo de tiempo;
- la introducción de nuevas tecnologías para reducir el riesgo o mitigar los impactos de las amenazas a la seguridad;
- los pasos dados para mejorar los medios existentes y su periodo de tiempo;
- la eliminación o la reducción de la frecuencia de incidentes particulares indeseados.

Las metas de seguridad deberían comunicarse (por ejemplo, sesiones de entrenamiento o de grupos foco; véase el numeral 4.4.2) al personal pertinente y deberían desplegarse a través de los programas de gestión de seguridad (véase el numeral 4.3.4).

e) Resultados típicos

Los resultados típicos incluyen metas de seguridad documentados y medibles donde sea factible, para cada función en la organización.

4.3.5 Programas de gestión de la seguridad

a) Requisito ISO 28000

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.

b) Propósito

Los programas de gestión de la seguridad deberían conectarse directamente a las metas y objetivos. Cada programa de gestión debería describir cómo la organización traducirá sus objetivos y compromisos de política en acciones definidas para que se logren las metas y objetivos de seguridad. El programa exigirá al desarrollo de estrategias y planes de acción que deberían emprenderse, los cuales deberían documentarse y comunicarse. El avance del programa con respecto a alcanzar el objetivo o los objetivos establecidos debería hacerse un seguimiento, revisarse y registrarse. La estrategia de disuasión y mitigación del programa debería basarse en los resultados provenientes de la amenaza de gestión de la seguridad y la identificación del riesgo y evaluación del riesgo (tales como el análisis de impacto, la evaluación del programa, la experiencia operacional).

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- metas y objetivos de seguridad;
- requisitos legales y otros;
- resultados de la identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo;

- detalles de las operaciones de la organización;
- información de la entrada de seguridad de los empleados, actividades de revisión y mejoramiento en el lugar de trabajo (estas actividades pueden ser de naturaleza reactiva o proactiva);
- revisión de oportunidades disponibles a partir de nuevas o diferentes opciones tecnológicas;
- actividades de mejoramiento continuo;
- disponibilidad de recursos necesarios para lograr los objetivos de seguridad de la organización.

d) Proceso

El programa de gestión de la seguridad debería definir:

- las responsabilidades por lograr los objetivos;
- los medios para lograr los objetivos:
- el marco de tiempo para lograr esos objetivos.

El programa debería considerar la mitigación de las amenazas a través de las opciones metodológicas y tecnológicas y la experiencia de otras entidades teniendo en cuenta los requisitos financieros, operacionales y comerciales así como las opiniones de las organizaciones similares y las partes interesadas.

Debería encargarse de la asignación de responsabilidad y autoridad apropiadas para cada tarea y debería asignar las escalas de tiempo para cada tarea individual, con el fin de cumplir con la escala de tiempo global del objetivo de seguridad relacionado. También debería encargarse de la asignación de los recursos adecuados (por ejemplo, financieros, humanos, de equipo, logísticos) para cada tarea.

Donde se esperen alteraciones o modificaciones significativas en las prácticas de trabajo, en los procesos, equipo o medios, el programa debería encargarse del ejercicio de nueva identificación de amenaza a la seguridad y de evaluación del riesgo. El programa de gestión de la seguridad debería encargarse de la consulta del personal pertinente acerca de los cambios esperados.

e) Resultados típicos

Los resultados típicos incluyen programas de gestión de la seguridad definidos y documentados para lograr los propósitos y objetivos descritos en los numerales 4.3.3 y 4.3.4.

4.4 IMPLEMENTACIÓN Y OPERACIÓN

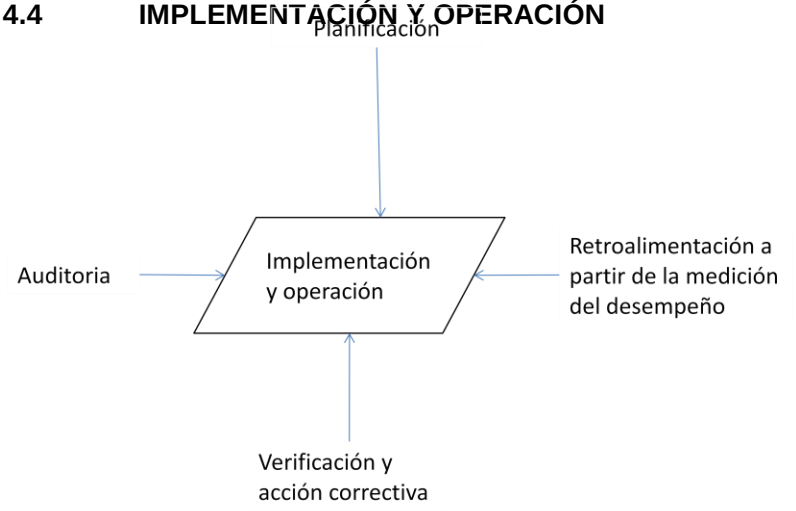

Figura 4. Implementación y operación

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

Requisito ISO 28000

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.

b) Propósito

Para facilitar la efectiva gestión de la segundad es necesario que se definan, documenten y comuniquen los roles, responsabilidades y autoridades, Sólo debería utilizarse personal de seguridad definido (véase la definición en la Cláusula 3) para tareas críticas de seguridad. Deberían proporcionarse los recursos adecuados para hacer posible que las tareas de seguridad se realicen.

c) Entradas típicas

Las entradas típicas incluyen lo siguiente:

- estructura organizacional;
- resultados de la identificación del riesgo de la seguridad, evaluación del riesgo y control del riesgo;
- metas, objetivos y programas de seguridad;
- requisitos legales y otros;
- descripciones del trabajo;
- listado de personal de seguridad calificado que necesita y/o ha recibido autorización en tareas de seguridad.

d) Proceso

1) Consideración general

Deberían definirse las responsabilidades y autoridad de todas las personas que cumplen deberes que son parte del sistema de gestión de la seguridad, incluyendo definiciones claras de responsabilidades en las interfases de las diferentes funciones.

Estas definiciones pueden ser exigidas, entre otras, por las siguientes categorías de personas:

- alta gerencia;
- nivel gerencial en toda la organización;
- los responsable de los contratistas y visitantes que tienen acceso a los predios y a sus empleados;
- los responsables del entrenamiento en seguridad;
- los responsables del equipo y operaciones que son críticos para la seguridad;
- los empleados que tienen autorización de seguridad u otros especialistas de seguridad dentro de la organización;
- los representantes de seguridad de los empleados en los foros consultivos.

Sin embargo, la organización debería comunicar y promover la idea de que la seguridad es responsabilidad de todos y cada uno en la organización, no sólo la responsabilidad de las personas que tienen deberes definidos en el sistema de gestión de la seguridad.

2) Definición de las responsabilidades de la alta gerencia

La responsabilidad de la alta gerencia debería incluir la definición de la política de seguridad de la organización y el aseguramiento de que el sistema de gestión de la seguridad se lleve a cabo. Como parte de este compromiso, debería designarse y nombrarse por la alta gerencia un determinado representante de la dirección con responsabilidades y autoridad para implementar el sistema de gestión de la seguridad. (En las grandes o muy complejas organizaciones puede haber más de un representante designado).

3) Definición de las responsabilidades del representante de la gestión de la seguridad

El representante de la gestión de la seguridad debería tener responsabilidad y autoridad para asegurar que el sistema de gestión de la seguridad se ¡triplemente y documente, tenga acceso permanente a la alta dirección y reciba apoyo de otro personal que ha delegado responsabilidades para el seguimiento de la operación general de la función de seguridad. El representante de la dirección debería ser informado con regularidad sobre el desempeño del sistema y debería mantener una participación activa en las revisiones periódicas y en el establecimiento de los objetivos de seguridad. Debería haber seguridad de que cualesquiera otros deberes o funciones asignadas a este personal no entre en conflicto con el cumplimiento de sus responsabilidades de seguridad.

4) Definición de las responsabilidades del nivel gerencia!

La responsabilidad del nivel gerencial debería incluir el aseguramiento de que la seguridad se maneje dentro de su área de operaciones. Donde la responsabilidad principal por asuntos de seguridad descansa en el nivel gerencial el rol y las responsabilidades de cualquier función de seguridad del especialista dentro de la organización deberían definirse apropiadamente para evitar ambigüedad con respecto a las responsabilidades y autoridades. Esto debería incluir acuerdos para resolver cualquier conflicto entre los aspectos de seguridad y las consideraciones de productividad por el ascenso a un nivel más alto de dirección.

5) Documentación de roles y responsabilidades

Las responsabilidades y autoridades de seguridad deberían documentarse en una forma apropiada para la organización. Esto puede tomar una o más de las siguientes formas o una alternativa de elección de la organización:

- manuales del sistema de gestión de la seguridad;
- procedimientos de trabajo y descripciones de la tarea;
- descripciones del trabajo;
- paquete de entrenamiento de inducción y programas de conocimiento.

Si la organización opta por emitir descripciones del trabajo escritas que cubran otros aspectos de los roles y responsabilidades de los empleados, entonces las responsabilidades de la seguridad deberían incorporarse a estas descripciones del trabajo.

6) Comunicación de roles y responsabilidades

Las responsabilidades y autoridades de la seguridad deberían comunicarse apropiadamente a aquellos a quienes afecten dentro de la organización. Esto debería asegurar que los individuos entiendan el alcance y las interfases entre las diversas funciones y los canales que van a usarse para comenzar la acción.

7) Recursos

La dirección debería asegurarse de que estén disponibles los recursos adecuados para el mantenimiento de una cadena de suministro segura, incluyendo equipo, recursos humanos, especialización y entrenamiento.

Los recursos pueden considerarse adecuados si son suficientes para llevar a cabo programas y actividades de seguridad, incluyendo la medición y supervisión del desempeño.

Para las organizaciones que tienen establecidos sistemas de gestión de la seguridad, la adecuación de recursos puede evaluarse al menos parcialmente comparando el logro planeado de los objetivos de seguridad con los resultados reales.

8) Compromiso de la dirección

Los gerentes deberían proporcionar una demostración visible de su compromiso con la seguridad. Los medios de demostración pueden incluir visitas e inspección a los sitios, participando en la investigación de incidentes de seguridad y proporcionando recursos en el contexto de la acción correctiva, asistencia a las reuniones de seguridad y envío de mensajes de apoyo.

e) Resultados típicos

Los resultados típicos incluyen lo siguiente:

- definiciones de las responsabilidades y autoridades de la seguridad para todo el personal pertinente;
- documentación de roles/responsabilidades en los manuales/procedimientos/ paquetes de entrenamiento;
- proceso para comunicar los roles y responsabilidades a todos los empleados y otras partes pertinentes;
- participación activa de la dirección y apoyo a la seguridad, a todos los niveles.

4.4.2 Competencia, entrenamiento y toma de conciencia

a) Requisito ISO 28000

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.

b) Propósito

Las organizaciones deberían tener procedimientos eficaces por asegurarse de que el personal es competente para llevar a cabo sus funciones de seguridad asignadas y ser conscientes de los riesgos de seguridad.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- definiciones de roles y responsabilidades;
- descripciones del trabajo (incluyendo detalles de las tareas de seguridad que van a realizarse);
- apreciaciones sobre el desempeño de los empleados;
- resultados de la identificación del riesgo de seguridad, evaluación del riesgo y control del riesgo;
- instrucciones sobre procedimientos y operaciones;
- política de seguridad y objetivos de seguridad;
- programas de seguridad.

d) Proceso

Los elementos siguientes deberían ser incluidos en el proceso:

- una identificación sistemática de la toma de conciencia y las competencias de seguridad que se requieren a cada nivel y función dentro de la organización;
- disposiciones para identificar y remediar cualquier déficit entre el nivel que posee actualmente el individuo y la toma de conciencia y competencia de seguridad que se requieren;
- provisión de cualquier entrenamiento identificado como necesario, de una manera oportuna y sistemática;
- evaluación de los individuos para asegurarse de que ellos han adquirido y mantienen el conocimiento y la competencia que se requieren;
- mantenimiento de registros apropiados del entrenamiento y competencia de un individuo.

NOTA Es importante que haya un fuerte énfasis en la toma de conciencia de la seguridad por parte de toda la organización para lograr un exitoso sistema de gestión de la seguridad y su implementación eficaz.

Debería establecerse y mantenerse un programa de toma de conciencia y entrenamiento en seguridad que apunte a las siguientes áreas:

- la toma de conciencia continua de los riesgos y amenazas de seguridad;
- una comprensión de los disposiciones de seguridad de la organización y de los roles y responsabilidades específicos de los individuos;
- un programa sistemático de inducción y entrenamiento continuo para los empleados y para quienes transfieren trabajos o tareas entre las divisiones, sitios, departamentos y áreas dentro de la organización;

- entrenamiento en las disposiciones de seguridad locales y riesgo de seguridad, riesgos, precauciones que deberían tomarse y procedimientos que deberían seguirse; este entrenamiento debería proporcionarse antes de comenzar el trabajo;
- entrenamiento para desempeñar identificación de riesgo de seguridad, evaluación del riesgo y control del riesgo (véase el numeral 4.31d);
- entrenamiento interno o externo específico que puede requerirse para los empleados que tienen roles específicos en el sistema de seguridad, incluyendo a los representantes de seguridad de los empleados;
- entrenamiento para todos los individuos que manejan empleados, contratistas y otros (por ejemplo, trabajadores temporales), en sus responsabilidades de seguridad. Esto con el fin de asegurarse de que tanto ellos como quienes están bajo *su* control entiendan las amenazas a la seguridad y los riesgos de las operaciones por las cuales son responsables, dondequiera que éstas tengan lugar. Además, con el fin de asegurarse de que el personal tiene las competencias necesarias para llevar a cabo las actividades seguramente, siguiendo los procedimientos de seguridad;
- los roles y responsabilidades (incluyendo responsabilidades legales individuales y corporativas) de la alta gerencia para asegurar que el sistema de gestión de la seguridad funciona para controlar los riesgos y minimizar las enfermedades, lesiones y otras pérdidas para la organización;
- programas de entrenamiento y conocimiento para contratistas, trabajadores temporales y visitantes, según el nivel de riesgo al que se exponen.

La efectividad de los programas de entrenamiento y toma de conciencia deberían evaluarse. Esto puede involucrar la evaluación como parte del ejercicio de entrenamiento y/o adecuados chequeos de campo para establecer si se ha logrado suficiente competencia y toma de conciencia o para el seguimiento del impacto a lo largo del plazo del entrenamiento efectuado.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- requisitos de competencia para los roles individuales;
- análisis de necesidades de entrenamiento;
- programas y planes de entrenamiento;
- gama de cursos y productos de entrenamiento disponible para uso dentro de la organización;
- registros de entrenamiento y registros de evaluación de la efectividad y del entrenamiento;
- programas de toma de conciencia de la seguridad;
- evaluación de la toma de conciencia de la seguridad.

4.4.3 Comunicación

a) Requisito ISO 28000

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.

b) Propósito

La organización debería estimular la participación en buenas prácticas de seguridad y apoyar su política de seguridad y objetivos de seguridad, a partir de todos los afectados por sus operaciones a través de un proceso de consulta y comunicación.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- política de seguridad y objetivos de seguridad;
- documentación del sistema pertinente de gestión de la seguridad;
- identificación del riesgo de seguridad, evaluación del riesgo y procedimientos de control del riesgo;
- definiciones de los roles y responsabilidades de la seguridad;
- resultados de las consultas de seguridad formales e informales de los empleados con la dirección;
- detalles del programa de entrenamiento;
- información pertinente, proveniente de las fuentes externas.

d) Proceso

La organización debería documentar y promover las disposiciones por las cuales consulta y comunica la información de seguridad pertinente a y de sus empleados y otras partes interesadas (por ejemplo, contratistas, visitantes, partes interesadas, socios comerciales, autoridades).

Esto debería incluir las disposiciones para involucrar a los empleados en los siguientes procesos:

- consulta sobre el desarrollo y revisión de políticas, el desarrollo y revisión de objetivos y decisiones de seguridad en la implementación de procesos y procedimientos para manejar los riesgos, incluyendo la realización de

evaluaciones de riesgo de seguridad y controles de riesgo pertinente a sus propias actividades;

- consulta sobre los cambios que afectan la seguridad del lugar de trabajo, como la introducción de nuevos o modificados equipos, medios, agentes químicos, tecnologías, procesos, procedimientos o patrones de trabajo.

Debería estimularse a los empleados para que hagan comentarios sobre aspectos de la seguridad y se les debería ser informados en especifico en la gestión de la cadena de mando para la seguridad.

e) Resultados típicos

Los resultados típicos incluyen lo siguiente:

- consultas formales a la dirección y a los empleados a través de consejos de seguridad o corporaciones similares;
- participación de los empleados en la identificación del riesgo de seguridad, evaluación del riesgo y control del riesgo;
- iniciativas para estimular consultas de seguridad de los empleados, actividades de revisión y mejora del lugar de trabajo y retroalimentación a la dirección sobre aspectos de seguridad;
- representantes de seguridad de los empleados con roles y mecanismos de comunicación definidos con la dirección, incluyendo, por ejemplo, la participación en investigaciones sobre accidentes e incidentes, inspecciones de seguridad del sitio, etc.;
- sesiones de información de seguridad para los empleados y otras partes interesadas; por ejemplo, contratistas o visitantes;
- carteleras de noticias que contengan información de seguridad;
- boletín de seguridad;
- programa de carteles de seguridad;
- otros medios para compartir información y reportes de seguridad sensible con las apropiadas autoridades y pares de la cadena de suministro.

4.4.4 Documentación

a) Requisito ISO 28000

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.

b) Propósito

La organización debería documentar y mantener documentación actualizada para asegurarse de que su sistema de gestión de la seguridad puede entenderse y llevarse a cabo y operar eficazmente.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- detalles de los sistemas de documentación e información que desarrolla la organización para apoyar su sistema de gestión de la seguridad y actividades de segundad y para cumplir con los requisitos de la norma ISO 28000;
- responsabilidades y autoridades;
- información sobre los medios en que se usa la documentación o la información y las restricciones que esto puede poner a la naturaleza física de la documentación o el uso de medios electrónicos u otros.

d) Proceso

La organización debería identificar los datos y la información que se necesitan para el sistema de gestión de la seguridad, antes de desarrollar la documentación necesaria para apoyar sus procesos de seguridad y su sistema de gestión de la seguridad.

No hay ningún requisito para desarrollar la documentación en un determinado formato a fin de cumplir con la norma ISO 28000, ni es necesario remplazar la documentación existente como manuales, procedimientos o instrucciones de trabajo si éstos describen adecuadamente las disposiciones actuales. Si la organización ya tiene un sistema de gestión de la seguridad establecido y documentado, puede demostrar que para ella es más conveniente y eficaz desarrollar, por ejemplo, un documento de referencia cruzada que describa la interrelación entre sus procedimientos existentes y los requisitos de la norma ISO 28000.

Debería tenerse en cuenta lo siguiente:

- las responsabilidades y autorizaciones de los usuarios de la documentación y la información, ya que esto debería llevar a determinar el grado de seguridad y accesibilidad que deberían imponerse;
- la manera en que se usa la documentación física y el ambiente en que se usa. Debería darse consideración similar respecto al uso de equipo electrónico para los sistemas de información.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- documento de apreciación global de la documentación del sistema de gestión de la seguridad;
- registros de documentos, listas maestras o índices;
- procedimientos;
- instrucciones de trabajo.

4.4.5 Control de documentos y datos

a) Requisito ISO 28000

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.

b) Propósito

Todos los documentos y datos que contienen información crítica para la operación del sistema de gestión de la seguridad y el desempeño de las actividades de seguridad de la organización, deberían identificarse y controlarse.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- detalles de los sistemas de documentación y de datos que la organización desarrolla para apoyar su sistema de gestión de la seguridad y las actividades de seguridad y para cumplir con los requisitos de la norma ISO 28000;
- detalles de las responsabilidades y autoridades.

d) Proceso

Los procedimientos escritos deberían definir los controles para la identificación, aprobación, emisión, acceso y eliminación de documentación de seguridad, junto con el control de seguridad de datos. Estos procedimientos deberían definir claramente las categorías de documentación y datos a los cuales se aplican y el nivel de clasificación con base en la sensibilidad sobre la seguridad.

La documentación y los datos deberían estar disponibles y accesibles al personal autorizado cuando se requiera, bajo condiciones de rutina y de no rutina, incluyendo emergencias.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimiento de control de documentos, incluyendo responsabilidades y autoridades asignadas;
- registros de documentos, listas maestras o índices;
- lista de documentación controlada y su localización;
- registros de archivos.

4.4.6 Control operacional

a) Requisito ISO 28000

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) y 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.

b) Propósito

La organización debería establecer y debería mantener disposiciones para asegurar la aplicación eficaz de medidas de control y de conteo, dondequiera que estas se requieran para controlar los riesgos de seguridad operacional, cumplir con la política y

los objetivos de seguridad, lograr las metas de seguridad y actuar conforme a los requisitos legales y otros.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- política de seguridad y objetivos de seguridad;
- identificación de amenazas a la seguridad y resultados de la evaluación del riesgo;
- requisitos legales, regulatorios y otros identificados.

d) Proceso

La organización debería establecer procedimientos para controlar sus riesgos identificados (incluyendo los que podrían provenir de contratistas, otros socios comerciales de la cadena de suministro o visitantes), documentando a éstos en los casos donde un falla en hacerlo pudiera ocasionar incidentes, emergencias u otras desviaciones de la política de seguridad y los objetivos de seguridad. Los procedimientos de gestión del riesgo deberían revisarse con regularidad para garantizar su conveniencia y efectividad, y los cambios que se identifican como necesarios deberían implementarse.

Los procedimientos deberían tomar en cuenta las situaciones en donde los riesgos se extienden a los intereses de los clientes u otras partes externas o áreas de control en otras partes de la cadena de suministro; por ejemplo, cuando los empleados de la organización están trabajando en el sitio de un cliente. A veces puede ser necesario entrar en consulta con la parte externa con respecto a la seguridad en tales circunstancias.

A continuación se indican algunos ejemplos de áreas en las que típicamente surgen riesgos y también algunos ejemplos de medidas de control contra ellos.

1) Compra o transferencia de bienes y servicios y uso de recursos externos

Esto incluye, por ejemplo, los siguientes elementos:

- evaluación y reevaluación periódica de la competencia de seguridad de los contratistas;
- aprobación del diseño de disposiciones de seguridad para nueva planta o equipo.

2) Tareas sensibles de seguridad

Esto incluye, por ejemplo, lo siguiente:

- identificación de tareas sensibles de seguridad;

- pre-determinación y aprobación de métodos de trabajo seguros;

- pre-calificación de personal para las tareas sensibles de seguridad;
- procedimientos de control de entrada de personal a las áreas sensibles de seguridad.

3) Mantenimiento del equipo de seguridad

Esto incluye lo siguiente:

- segregación y control de acceso;
- inspección y prueba equipo relacionado con la seguridad y sistemas de alta integridad.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimientos;

- instrucciones de operación y mantenimiento.

4.4.7 Preparación y respuesta ante emergencias y recuperación de la seguridad

a) Requisito ISO 28000

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.

b) Propósito

La preparación, respuesta y recuperación que siguen a un incidente de seguridad son cubiertas por este numeral. El término preparación para la emergencia significa los planes, preparaciones y acciones preventivas que se implementan siguiendo eventos o crisis de seguridad no planeados.

La organización debería evaluar activamente las necesidades de incidente potencial y respuesta para todos los potenciales eventos de seguridad identificados a través del proceso de identificación de la amenaza y de evaluación del riesgo (véase el numeral 4.3.1). Deberían desarrollarse planes de respuesta, procedimientos y

procesos para afrontarlos, respuestas planeadas de prueba y búsqueda de mejoramiento de la efectividad de sus respuestas.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- identificación de amenazas a la seguridad y evaluación del riesgo;
- disponibilidad de servicios de emergencia locales y agencias de seguridad y detalles de cualquier respuesta de emergencia o arreglos de consulta que han sido acordados;
- requisitos regulatorios, legales u otros;
- experimenta y revisión de incidentes previos y situaciones de emergencia y los resultados de las acciones subsiguientes;
- experiencias similares de las organizaciones a partir de previos incidentes y situaciones de emergencia (lecciones aprendidas, mejores prácticas);

- policía, inteligencia y entrada de primeros respondientes;

- revisión de la práctica, ejercicios y adiestramiento realizados.

d) Proceso

La organización debería desarrollar un plan de emergencia, identificar y proporcionar apropiadas disposiciones de emergencia y probar con regularidad su capacidad a través de ejercicios de práctica. Los planes de preparación para la emergencia, respuesta y recuperación de la seguridad deberían incluir medidas para restaurar la seguridad, proteger los datos y los medios y asegurar la continuidad de la seguridad.

Los ejercicios de práctica deberían poner a prueba la efectividad de las partes más críticas del plan de respuesta de seguridad y la integridad del proceso de planeación de emergencia. Aunque los ejercicios en computador pueden ser útiles durante el proceso de planificación, deberían efectuarse ejercicios y adiestramiento de práctica realista. Deberían evaluarse los resultados del adiestramiento y práctica de emergencias y deberían implementarse los cambios que se identifiquen como necesarios.

1) Respuesta de emergencia y plan de recuperación de seguridad

La respuesta de emergencia y el plan de recuperación de seguridad deberían esbozar las acciones que se van a tomar cuando surjan situaciones específicas y deberían incluir lo siguiente:

- identificación de incidentes y emergencias potenciales;
- identificación de la persona que tomará el cargo durante la emergencia;
- detalles de las acciones que tomará el personal durante una emergencia, incluyendo las acciones que tomará el personal externo que está en el sitio de la emergencia, como contratistas o visitantes (de quienes se

puede requerir, por ejemplo, que se trasladen a puntos específicos de reunión de evacuación);

- la responsabilidad, la autoridad y los deberes del personal que tiene roles específicos durante la emergencia (por ejemplo, seguridad, vigilancia contra incendios, personal de primeros auxilios, especialistas en contaminación radiológica o tóxica);
- procedimientos de evacuación;
- procedimientos que describen cómo se reintegran las medidas de seguridad y las condiciones seguras a corto y mediano plazos;
- identificación, localización y protección de materiales de seguridad, registros, datos y equipo y acción de emergencia que se requieran;
- interfaz con la servicios de emergencia y primeros respondientes; comunicación con las partes interesadas;
- disponibilidad de la información necesaria durante la emergencia; por ejemplo, dibujos de diseño de planta, datos de seguridad, procedimientos, instrucciones de trabajo y números de teléfonos de contacto;
- interfaz y comunicación con otros pares de la cadena de suministro del negocio /de comercio;
- asegurar la integridad de los sistemas de comunicación.

La participación de agencias externas en la planeación y respuesta de emergencia debería documentarse claramente. Estas agencias deberían ser aconsejadas acerca de las posibles circunstancias de su participación y se les debería proporcionar dicha información a medida que requieran facilitar su participación en las actividades de respuesta.

2) Equipo de seguridad

Deberían identificarse las necesidades de equipo de seguridad y debería proporcionarse el equipo en la cantidad adecuada. Esto debería probarse a intervalos de tiempo especificados para continuar la operabilidad.

3) Simulacros y ejercicios de práctica

El simulacro y los ejercicios de práctica deberían llevarse a cabo de acuerdo con un marco de tiempo predeterminado. Donde sea apropiado y factible, debería estimularse la participación de servicios externos de seguridad en los simulacros y ejercicios de práctica.

e) Resultados típicos

Los resultados típicos incluyen lo siguiente:

- planes y procedimientos documentados de respuesta ante emergencias y de recuperación de la seguridad;
- lista de equipo de seguridad; registros de prueba para el equipo de seguridad;
- simulacros y ejercicios de práctica;
- revisiones de los simulacros y ejercicios de práctica;
- acciones recomendadas que surgen de las revisiones;
- avance frente al logro de acciones recomendadas;
- acciones completadas.

4.5 VERIFICACIÓN Y ACCIÓN CORRECTIVA

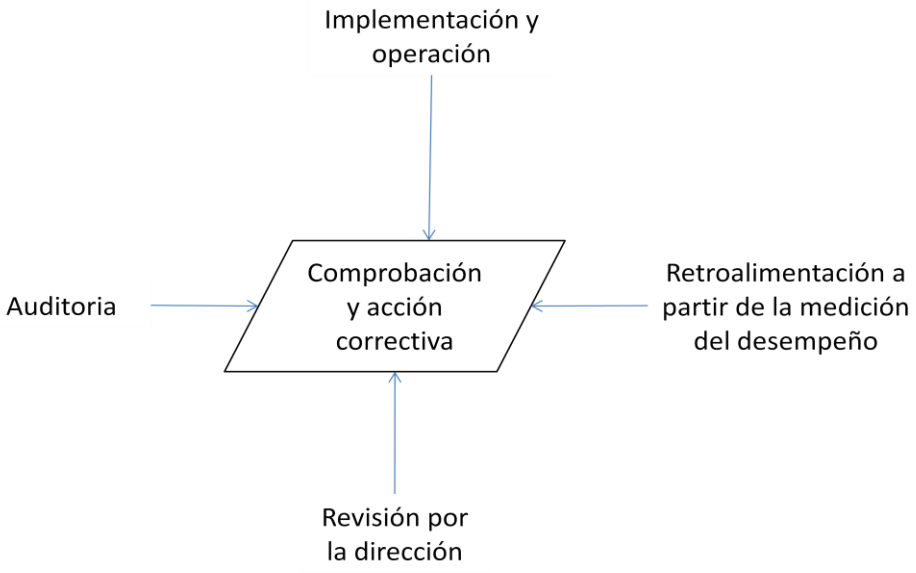

Figura 5. Comprobación y acción correctiva

4.5.1 Medición y seguimiento del desempeño de seguridad

a) Requisito ISO 28000

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.

b) Propósito

La organización debería identificar los indicadores clave de desempeño para su desempeño de seguridad a través de toda la organización y de la cadena de suministro que controla o sobre la cual tiene influencia. Éstos deberían incluir, pero no limitarse a, el indicador medible que determina si:

- están lográndose la política de seguridad y los objetivos de seguridad;
- están controlándose las amenazas y/o están mitigándose, por cuanto se han implementado apropiadas medidas preventivas y éstas han sido eficaces;
- las lecciones están siendo aprendidas a partir de las fallas del sistema de gestión de seguridad, incluyendo incidentes de seguridad y posibles pérdidas;
- los programas de toma de conciencia, entrenamiento, comunicación y consulta para los empleados y partes interesadas son eficaces;
- la información que puede usarse para revisar y mejorar aspectos del sistema de gestión de seguridad está produciéndose y utilizándose.

c) Entradas típicas

Las entradas típicas incluyen lo siguiente:

- identificación de amenazas a la seguridad, evaluación del riesgo y gestión del riesgo (véase el numeral 4.3.1);

- requisitos de legislación, regulaciones, las mejores prácticas (si las hubiere);
- política de seguridad y objetivos de seguridad;
- procedimiento para manejar no conformidades;
- prueba de equipos de segundad y registros de calibración (incluyendo los que pertenecen a contratistas);
- registros de entrenamiento (incluyendo los que pertenecen a contratistas);
- informes de dirección.

d) Proceso

1) Seguimiento proactivo y reactivo

El sistema de gestión de la seguridad de una organización debería incorporar seguimiento proactivo y reactivo como sigue:

- debería usarse seguimiento proactivo para verificar la concordancia con las actividades de seguridad de la organización; por ejemplo, seguimiento de la frecuencia y efectividad de las inspecciones de seguridad;
- el seguimiento reactivo debería usarse para investigar, analizar y registrar las fallas del sistema de gestión de la seguridad, incluyendo emergencias e incidentes de seguridad.

Los datos tanto del seguimiento proactivo como del reactivo se usan a menudo para determinar si se alcanzan los objetivos de seguridad.

2) Técnicas de medición

Los siguientes son algunos ejemplos de métodos que pueden emplearse para medir el desempeño de la seguridad:

- resultados de los procesos de identificación de riesgo de la seguridad, evaluación del riesgo y control del riesgo, así como el cumplimiento del Marco de Normas WCO SAFE y del *United States' Customs - Trade Partnership Against Terrorísm (C-TPAT) y la regulación del European Commission Authorized Economic Operator (AEO);*
- inspecciones sistemáticas usando listas de control;
- inspecciones de seguridad;
- evaluación de nuevos sistemas de logística de la cadena de suministro;
- revisión y evaluación de los modelos estadísticos de logística resultantes;
- inspecciones del equipo de seguridad para verificar que esté en buenas condiciones;

- disponibilidad y efectividad del empleo de personal que tenga reconocida experiencia de seguridad o calificaciones formales;
- muestreo de comportamiento: evaluación del comportamiento de los trabajadores para identificar prácticas de seguridad deficientes que podrían requerir corrección;
- análisis de documentación y registros;
- *"Benchmarking"* frente a la buena práctica de seguridad de otras organizaciones;
- inspecciones para determinar las actitudes del empleado a fin de descubrir comportamientos sospechosos;
- retroalimentación de las partes interesadas.

Las organizaciones deberían decidir a qué van a hacer seguimiento y con qué frecuencia van a hacerlo, con base en el nivel de riesgo (véase el numeral 4.3.1). Un marco de tiempo para las inspecciones basado en la identificación de amenaza a la seguridad y en los resultados de la evaluación del riesgo, la legislación y las regulaciones, debería prepararse como parte del sistema de gestión de la seguridad.

El seguimiento de los procesos de seguridad de rutina, nodos de logística, socios comerciales, actividades y prácticas de la cadena de suministro, deberían llevarse a cabo de acuerdo con un documentado esquema de seguimiento por personal autorizado, que también debería emprender chequeos de inconvenientes de tareas críticas para asegurar la concordancia con los procedimientos de seguridad y códigos de práctica. Para ayudar a realizar las inspecciones y seguimiento sistemáticos, pueden usarse listas de control.

3) Equipo de seguridad

El equipo de seguridad que se usa para hacer seguimiento a la seguridad y garantizarla (por ejemplo, cámaras, cercos, puertas, alarmas, etc.) debería listarse, identificarse en su especificidad y controlarse. La exactitud de este equipo debería conocerse. Donde sea necesario, debería disponerse de procedimientos por escrito en los que se describa cómo se realizan las medidas de seguridad. Los equipos usados para la seguridad deberían mantenerse de una manera apropiada y estar en capacidad de funcionar tal como se requiere.

Debería documentarse e implementarse un esquema de calibración y mantenimiento para el equipo de seguridad cada vez que se requiera. Este esquema debería incluir los siguientes elementos:

- la frecuencia de la calibración y el mantenimiento;
- referencia a los métodos de prueba, donde sea aplicable hacerlo;
- identidad del equipo que va a usarse para la calibración;
- acción que va a efectuarse cuando el equipo de seguridad especificado se encuentra fuera de calibración.

La calibración y el mantenimiento deberían llevarse a cabo bajo las condiciones apropiadas. Deberían prepararse los procedimientos adecuados para las calibraciones críticas o difíciles.

El equipo usado para hacer la calibración debería ser acorde con las normas nacionales donde tales normas existan. Si no existe dicha norma, debería documentarse la base para aplicar los correspondientes niveles usados.

Deberían mantenerse registros de todas las calibraciones, actividades de mantenimiento y resultados. Los registros deberían dar detalles de las mediciones efectuadas antes y después del ajuste.

Deberían identificarse claramente a los usuarios los estados de calibración del equipo de seguridad.

El equipo de seguridad cuyo estado de calibración o de mantenimiento se desconoce o se sabe que está fuera de calibración, no debería usarse. Adicionalmente, debería ponerse fuera de uso y señalarse claramente, mediante etiqueta u otra clase de marca, para prevenir el mal uso. Dicha marca debería ser acorde con los procedimientos escritos. Los procedimientos deberían incluir la identificación del estado de calibración del producto. Debería emitirse una nota de no conformidades para documentar las acciones tomadas. Los procedimientos deberían incluir un plan de acción si se descubre equipo que esté fuera de calibración.

4) Inspecciones

i) Equipo

Debería esbozarse un inventario (usando identificación única de todos los elementos) de todo el equipo de seguridad. Dicho equipo debería inspeccionarse como se requiere e incluirse en los esquemas de inspección.

ii) Inspecciones de seguridad

Deberían llevarse a cabo inspecciones de seguridad, pero estas no deberían eximir el personal autorizado de efectuar inspecciones regulares o de identificar las amenazas a la seguridad.

iii) Registros de la inspección

Debería mantenerse un registro de cada inspección de seguridad llevada a cabo. Los registros deberían indicar si los procedimientos de seguridad documentados estaban acordes o no. Los registros de inspecciones de seguridad, giras, sondeos y auditorías del sistema de gestión de la seguridad deberían tener muestreo para identificar causas subyacentes de no conformidades y riesgo de seguridad repetitivo. Debería tomarse cualquier acción preventiva que sea necesaria. Las situaciones de amenaza a la seguridad y el equipo no consistente identificado durante las inspecciones debería documentarse como no conformidad, evaluado como de riesgo y corregido de acuerdo con el procedimiento de no conformidades.

5) Equipo del proveedor (contratista)

Los equipos de seguridad usados por contratistas deberían estar sujetos a los mismos controles que el equipo interno. Debería exigirse a los contratistas que den garantías de que su equipo concuerda con estos requisitos. Antes de comenzar el trabajo, el proveedor debería proporcionar una copia de sus registros de prueba y mantenimiento del equipo para cualquier equipo crítico identificado que requiera dichos registros. Si alguna de las tareas requiere entrenamiento especial, deberían suministrarse al cliente los correspondientes registros de entrenamiento para su revisión.

6) Técnicas analíticas estadísticas u otras técnicas teóricas

Cualquier técnica analítica estadística u otra técnica teórica empleada para evaluar una situación de seguridad, investigar un incidente o falla de seguridad o para ayudar en la toma de decisiones respecto de la seguridad debería basarse en principios científicos reconocidos. La alta gerencia debería asegurarse de que se ha identificado la necesidad de dichas técnicas. Donde sea apropiado, deberían documentarse pautas para su uso, junto con las circunstancias en que estas son apropiadas.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimiento(s) para el seguimiento de la efectividad de las disposiciones de seguridad;
- cronogramas de inspección y listas de control;
- listas de control de inspección de equipo;
- lista de equipo de seguridad;
- disposiciones de calibración y registros de calibración;
- actividades y resultados de mantenimiento;
- completas listas de control e informes de inspección (resultados de auditoría del sistema de gestión de la seguridad (véase el numeral 4.5.4);
- informes sobre no conformidades;
- evidencia de los resultados de la implementación de dicho(s) procedimiento(s).

4.5.2 Evaluación del sistema a)

Requisito ISO 28000

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.

b) Propósito

Las organizaciones deberían tener procedimientos eficaces para revisar y evaluar los planes de gestión de la seguridad, los procedimientos y capacidades de la organización para cumplir su política y metas y objetivos. La organización debería también revisar periódicamente su cumplimiento con los requisitos regulatorios aplicables.

El propósito principal de estos procedimientos es asegurar que los planes y procedimientos de seguridad se mantengan actualizados y en concordancia con los cambiantes requisitos y necesidades. Estos cambios deberían ser oportunos y tomar plenamente en cuenta cualquier cambio en las regulaciones de la cadena de suministro, las mejores prácticas y las lecciones aprendidas.

c) Entradas típicas

Las entradas típicas deberían incluir:

- los informes de incidentes; los resultados de los ejercicios de planificación y preparación para incidentes;
- la identificación de amenazas, y los informes de evaluación del riesgo y control del riesgo;
- los informes de auditoría del sistema de gestión de la seguridad, incluyendo los informes de no conformidades;
- los informes de incidentes y/o riesgos;
- los informes y acciones de revisión de la dirección (véase el numeral 4.6);
- el avance en el logro de los objetivos;
- los requisitos regulatorios cambiantes;

- las expectativas cambiantes de las partes involucradas y las partes interesadas;
- los cambios en el alcance del trabajo, actividades y base de clientes de las organizaciones.

d) Proceso

La dirección de la organización debería efectuar revisiones, a intervalos apropiados, de su sistema de gestión de la seguridad para establecer y asegurar su continua conveniencia y efectividad. Los intervalos deberían ser suficientemente cortos que para que puedan identificarse las fallas de los sistemas antes de que surjan los consiguientes daños y perjuicios.

El resultado de sistemas eficaces y de su implementación, el logro del objetivo y de la política con el mejoramiento continuo ha de ser uno de los principios que se desprendan de la norma ISO 28000. El proceso y los procedimientos exigidos por el numeral 4.5.2 asegurarán que esto se logre.

e) Resultados típicos

Los resultados típicos incluyen:

- procesos y desempeño mejorados;
- reducción de los informes de no conformidades;
- cumplimiento legal;
- actualización de la identificación de amenazas, evaluación del riesgo y registros de riesgo;
- procesos mejorados;
- evidencia de las evaluaciones de la eficacia de las acciones correctivas y preventivas tomadas.

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

a) Requisito ISO 28000

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 segundad 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.

b) Propósito

Las organizaciones deberían tener procedimientos eficaces para informar y evaluar y/o investigar emergencias, incidentes de seguridad e y no conformidades. El principal propósito del o de los procedimientos es prevenir la posterior ocurrencia de la situación, identificando y manejando la(s) causa(s) originales. Además, los procedimientos deberían posibilitar la detección, análisis y eliminación de causas potenciales de no conformidades, incluyendo las que resultan de fallas y errores humanos, del sistema, proceso o equipo.

c) Entradas típicas

- Las entradas típicas incluyen los siguientes elementos:

procedimientos (en general); plan de emergencia;

- identificación de amenazas a la segundad, evaluación del riesgo y gestión del riesgo;
- informes de auditoría del sistema de gestión de la seguridad, incluyendo informes de no conformidades;
- incidentes de seguridad e informes de amenaza a la seguridad; informes de

mantenimiento y servicio para el equipo de seguridad.

d) Proceso

Se exige a la organización preparar procedimientos documentados para garantizar que se investiguen los incidentes y las no conformidades de seguridad y que se inicien

acciones correctivas y/o preventivas. El avance en la aplicación de acciones correctivas y preventivas debería tener seguimiento y debería revisarse la eficacia de dichas acciones.

1) Procedimientos

Los procedimientos deberían incluir la consideración de los siguientes elementos:

i) General

El procedimiento debería:

- definir las responsabilidades y la autoridad de las personas involucradas en la implementación, informe, investigación, seguimiento y supervisión de las acciones correctivas y preventivas;
- exigir que se informen todas las no conformidades, incidentes de seguridad y amenazas a la seguridad;
- aplicarse a todo el personal (es decir, empleados, trabajadores temporales, contratistas, visitantes y cualquier otra persona involucrada en la cadena de suministro);
- tener en cuenta los impactos en las partes interesadas;
- garantizar que no se critique *a* ningún empleado por informar incidentes de seguridad;
- definir claramente el curso de acción que se va a tomar siguiendo las no conformidades identificadas en el sistema de gestión de seguridad.

ii) Acción inmediata

La acción inmediata para corregir el incidente de seguridad debería tomarse cuando se han identificado primero las no conformidades, los incidentes de seguridad o las amenazas a la seguridad. Los procedimientos deberían:

- definir el proceso de notificación;
- donde corresponda, incluir la coordinación con los planes y procedimientos de emergencia;
- definir la escala del esfuerzo investigativo con respecto a la amenaza potencial o real (por ejemplo, incluir a la administración in la investigación de incidentes de seguridad serios);

iii) Registro

Deberían emplearse los medios apropiados para registrar la información factual y los resultados de la investigación inmediata y la subsiguiente

Investigación detallada. La organización debería garantizar que se sigan los procedimientos para:

- registrar los detalles de la no conformidad, el incidente de segundad o las amenazas a la seguridad;
- definir dónde se van a almacenar los registros y la responsabilidad por este almacenamiento.

iv) Investigación

Los procedimientos deberían definir la manera como debería manejarse el proceso de investigación. Los procedimientos deberían identificar:

- el tipo de eventos que se van a investigar (por ejemplo, incidentes que pudieran haber ocasionado una seria amenaza);
- el propósito de las investigaciones;
- quién va a investigar, la autoridad de los investigadores, las calificaciones requeridas (incluyendo la dirección de línea cuando corresponda);
- la causa original de la no conformidad;
- las disposiciones para entrevistas a testigos;
- aspectos prácticos como la disponibilidad de cámaras y almacenamiento de evidencia;
- disposiciones sobre informe de la investigación, incluyendo informes a las partes interesadas apropiados.

El personal investigador debería empezar su análisis preliminar de los hechos mientras se reúne información más extensa. La recolección de datos y el análisis deberían continuar hasta que se obtenga una explicación adecuada y suficientemente amplia.

v) Acción correctiva

Las acciones correctivas son las acciones que se toman para identificar la(s) causa(s) originales de las no conformidades e incidentes de seguridad y dar los pasos necesarios para prevenir que se repitan. Entre los ejemplos de elementos que se van a considerar a fin de establecer y mantener los procedimientos de acción correctiva están:

- la identificación e implementación de medidas correctivas y preventivas tanto para corto plazo como para largo plazo (esto también puede incluir el uso de fuentes de información apropiadas, como el consejo de empleados que tienen especialización en seguridad);

- la evaluación de cualquier impacto en la identificación de amenaza a la seguridad y los resultados de la evaluación del riesgo [y cualquier necesidad de actualizar la identificación de amenaza a la seguridad, evaluación del riesgo e informe(s) de gestión del riesgo];
- el registro de cualquier cambio que se requiera en los procedimientos resultantes de la acción correctiva o la identificación de amenaza a la seguridad, evaluación y gestión del riesgo;
- aplicación de la gestión del riesgo o modificación de la gestión del riesgo existente, para asegurar que se tomen las acciones correctivas y que estas sean eficaces.

Vi) Acción preventiva

Las acciones preventivas son las acciones que se toman para impedir que ocurran potenciales no conformidades de seguridad. Ejemplos de elementos por considerar al establecer y mantener procedimientos de acción preventiva son los siguientes:

- el uso de fuentes de información apropiadas, como los resultados de las acciones correctivas, tendencias de incidentes de seguridad, informes de auditoría del sistema de gestión de seguridad, evaluaciones de riesgo actualizadas, nueva información sobre seguridad, consejo de los empleados y partes interesadas que tienen especialización en seguridad, etc.
- iniciación e implementación de acción preventiva y la aplicación de controles para garantizar que sea eficaz;
- registro de cualquier cambio en los procedimientos resultantes de la acción preventiva y sometimiento a aprobación.

vii) Seguimiento

La acción correctiva o preventiva que se tome debería ser tan eficaz como sea factible. Deberían hacerse chequeos sobre la efectividad de la acción correctiva/preventiva tomada. Las acciones pendientes/no cumplidas deberían informarse a la dirección a la más temprana oportunidad.

2) Análisis de la no conformidad e incidente de seguridad

Las causas de las no conformidades e incidentes de seguridad deberían clasificarse y analizarse sobre una base regular para posibilitar un análisis de la causa original. Los indicadores de frecuencia y severidad deberían marcarse con otros integrantes de la cadena de suministro.

En la clasificación y análisis debería incluirse lo siguiente:

- reportes de frecuencia o tasas de severidad de los incidentes de seguridad;

- localización, actividad involucrada, agencia involucrada, día, momento del día (cualquiera que corresponda);
- tipo y grado de impacto sobre los medios, la cadena de suministro, etc.;
- causas directas y de origen.

Debería prestarse la debida atención a los incidentes de seguridad. Todos los incidentes de seguridad podrían ser un indicador de una amenaza o vulnerabilidad de seguridad.

Deberían derivarse conclusiones válidas y tomarse una acción correctiva. Este análisis debería enviarse a la alta dirección e incluirse en la revisión por la dirección (véase el numeral 4.6).

3) Resultados del seguimiento y la comunicación

Debería evaluarse la efectividad de las investigaciones e informes de seguridad. La evaluación debería ser objetiva y debería arrojar un resultado cuantitativo donde sea posible.

La organización, habiendo aprendido de la investigación, debería:

- identificar las causas originales de las deficiencias del sistema de gestión de la seguridad y de la gestión general de la organización dónde corresponda;
- comunicar los resultados y recomendaciones a la dirección y a las partes interesadas pertinentes (véase el numeral 4.4.3);
- incluir los resultados y recomendaciones pertinentes de las investigaciones en el proceso continuo de revisión de la seguridad;
- hacer seguimiento a la implementación oportuna de controles remédiales y a su subsiguiente efectividad con el tiempo;
- aplicar las lecciones aprendidas de la investigación de los incidentes y no conformidades de seguridad a través de su organización en general, la cadena de suministro que controla y sobre la cual tiene influencia, centrándose en los amplios principios involucrados, en vez de restringirse a la acción específica diseñada para evitar la repetición de un evento que es precisamente similar en la misma área de la organización.

4) Mantenimiento de registro

Este puede cumplirse rápidamente y con un mínimo de planificación formal o puede ser una actividad más compleja y a largo plazo. La documentación asociada debería ser apropiada al nivel de acción correctiva.

Deberían enviarse informes y sugerencias al representante de la alta gerencia para efectos de análisis y retención (véase el numeral 4.5.4).

La organización debería mantener un registro de incidentes de seguridad. Dichos registros pueden ser exigidos por los reguladores de la cadena de suministro.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimiento sobre incidente de seguridad y no conformidad; informes sobre

  no conformidades; registro de no conformidades; informes de investigación;
- informes actualizados sobre identificación de riesgo de seguridad, evaluación del riesgo y gestión del riesgo;
- entrada de revisión de la dirección;
- evidencia de evaluaciones de la eficacia de las acciones correctivas y preventivas tomadas.

4.5.4 Control de registros

a) Requisito ISO 28000

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.

b) Propósito

Deberían mantenerse registros para demostrar que el sistema de gestión de la seguridad opera eficazmente. Deberían prepararse, mantenerse, ser legibles y estar adecuadamente identificados, los registros de seguridad que soportan el sistema de gestión y su conformidad con los requisitos.

c) Entradas típicas

Entre los registros que deberían mantenerse (utilizados para demostrar la conformidad con los requisitos) están los siguientes:

- registros de entrenamiento y competencia;
- informes de inspección de seguridad;
- no conformidades de seguridad;
- resultados de las acciones preventivas y correctivas;
- informes de auditoría del sistema de gestión de la seguridad;
- actas de las reuniones de seguridad;
- informas de ejercicios de seguridad y adiestramiento;
- revisiones por la dirección;
- registros de identificación de amenazas a la seguridad, evaluación del riesgo y gestión del riesgo.

d) Proceso

El requisito de la norma ISO 28000 es bastante autoexplicativo. Sin embargo, también debería darse consideración adicional a los siguientes elementos:

- la autoridad para la disposición de los registros de seguridad;
- la confidencialidad (marcas de protección) de los registros de seguridad;
- requisitos legales y otros sobre retención de los registros de seguridad;
- aspectos que rodean el uso de registros electrónicos.

Los registros de seguridad deberían rellenarse totalmente, e identificarse de manera legible y adecuada. Deberían definirse los registros de seguridad para los tiempos de retención. Los registros deberían mantenerse en un lugar seguro, poder recuperarse prontamente y estar protegidos contra el deterioro. Los registros de seguridad críticos deberían protegerse de posible fuego y cualquier otro daño como corresponda y como exija la ley.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- procedimiento (para la identificación, mantenimiento y disposición de los registros de seguridad);
- registros de seguridad guardados adecuadamente y prontamente recuperables.

4.5.5 Auditoría

a) Requisito ISO 28000

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.

b) Propósito

Las auditorías internas del sistema de gestión de la seguridad de una organización deberían efectuarse a intervalos planeados para determinar y proporcionar información a la dirección acerca de si el sistema concuerda con los requisitos de procedimiento y los requisitos de la totalidad del numeral 4 de la norma ISO 28000:2007 y si se han implementado y mantenido apropiadamente. También pueden realizarse para identificar oportunidades para el mejoramiento del sistema de gestión de la seguridad de una organización. En general, las auditorías del sistema de gestión de la seguridad deberían considerar la política y los procedimientos de seguridad así como las condiciones y prácticas aplicables a la cadena de suministro.

Debería establecerse un programa de auditoría interna del sistema de gestión de la seguridad para permitir a la organización revisar su propia concordancia de su sistema de gestión de la seguridad con los requisitos de la norma ISO 28000 y otros según lo definido dentro del alcance de sus operaciones. Las auditorías planeadas del sistema

de gestión de la seguridad deberían llevarse a cabo por personal del interior de la organización y/o por personal externo escogido por la organización, a fin de establecer el grado de concordancia con los procedimientos de seguridad documentados y evaluar si el sistema es eficaz o no en cumplir con los objetivos de seguridad de la organización. El personal que dirige las auditorías del sistema de gestión de la seguridad debería ser capaz de hacerlo de manera imparcial y objetiva.

NOTA Las auditorías internas del sistema de gestión de la seguridad se centran en el desempeño del sistema de gestión de la seguridad, y no deberían confundirse con las evaluaciones o revisiones de seguridad u otras inspecciones de seguridad.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- declaración de la política de seguridad; objetivos de seguridad; procedimientos e instrucciones de seguridad;
- resultados de la identificación de amenazas a la seguridad, evaluación del riesgo y gestión del riesgo;
- legislación y mejores prácticas (si se aplican);
- informes de no conformidades;
- procedimientos de auditoría del sistema de gestión de la seguridad;
- auditor o auditores competentes, independientes, internos o externos;
- procedimiento sobre no conformidades;
- ejercicios y adiestramiento de seguridad;
- información de amenaza a la segundad por parte de agencias externas.

d) Proceso

1) Auditorías

Las auditorías del sistema de gestión de la seguridad proporcionan una evaluación amplia y formal de la concordancia con los procedimientos y prácticas de seguridad de la organización.

Las auditorías del sistema de gestión de la seguridad deberían dirigirse de acuerdo con las disposiciones planeadas. Deberían realizarse auditorías adicionales según lo requieran las circunstancias. Por ejemplo, después de los incidentes que impactan en el sistema de seguridad, los cambios en la organización o los medios o el alcance de la cadena de suministro.

Las auditorías del sistema de gestión de la seguridad sólo deberían llevarse a cabo por personal competente e independiente, con las apropiadas autorizaciones de seguridad para las áreas que se están auditando.

El resultado de la auditoría del sistema de gestión de la seguridad debería incluir evaluaciones detalladas de la efectividad de los procedimientos de seguridad, el nivel de cumplimiento con los procedimientos y prácticas y además debería identificar las acciones correctivas donde sea necesario. Los resultados de las auditorías del sistema de gestión de la seguridad deberían registrarse e informarse a la dirección, de una manera oportuna.

NOTA Los principios generales y la metodología descritos en la norma ISO 19011 son apropiados para la auditoría del sistema de gestión de la seguridad.

2) Cronograma

Debería prepararse un plan, normalmente anual, que indique el cronograma de auditorías internas del sistema de gestión de la seguridad. Las auditorías del sistema de gestión de la seguridad deberían apuntar hacia todas las operaciones cubiertas por el sistema de gestión de la seguridad y evaluar su conformidad con la norma ISO 28000.

La frecuencia y el cubrimiento de las auditorías del sistema de gestión de la seguridad deberían estar correlacionados con los riesgos asociados a los diversos elementos del sistema de gestión de la seguridad, los datos disponibles sobre el desempeño del sistema de gestión de la seguridad, el resultado de las revisiones por la dirección y la medida en que el sistema de gestión de la seguridad o el ambiente en que opera están sujetos al cambio.

Deberían dirigirse auditorías adicionales, no programadas, del sistema de gestión de la seguridad, si ocurren situaciones que las ameriten; por ejemplo, después de un incidente de seguridad.

3) Apoyo de la dirección

Para que la auditoría de los sistemas de gestión de la seguridad sea de valor es necesario que la alta gerencia esté plenamente comprometida con el concepto de auditoría y su implementación eficaz dentro de la organización. La alta gerencia debería someter a consideración los resultados y recomendaciones de la auditoría y tomar acciones apropiadas según sea necesario, dentro de un tiempo apropiado. Una vez se ha convenido que debería llevarse a cabo una auditoría del sistema de gestión de la seguridad, esta debería completarse de una manera imparcial. Todo el personal pertinente debería ser informado de los propósitos de la auditoría y de los beneficios de la misma. Se debería instar al personal a cooperar plenamente con los auditores y responder honesta y constructivamente a sus preguntas.

4) Los auditores

Una o más personas pueden emprender las auditorías del sistema de gestión de la seguridad. Un enfoque de equipo puede ensanchar la participación y mejorar la cooperación. Un enfoque de equipo también puede posibilitar que se utilice una gama más amplia de habilidades y conocimiento especializados.

Los auditores deberían ser independientes de la parte de la organización o de la actividad que va a ser auditada y, si es necesario, deberían recibir autorización de seguridad para las áreas que se estén auditando.

Los auditores deberían entender su tarea y ser competentes para llevarla a cabo. Deberían tener la experiencia y el conocimiento de las normas, códigos de práctica y sistemas pertinentes que están interviniendo, de tal modo que les permitan evaluar el desempeño e identificar las deficiencias. Los auditores deberían estar familiarizados con los requisitos establecidos en cualquier legislación pertinente. Además, deberían ser conscientes de las normas y pautas de autoridad pertinentes al trabajo en que están comprometidos y tener acceso a ellas.

5) Recolección e interpretación de datos

Las técnicas y ayudas usadas en la recolección de la información dependerán de la naturaleza de la auditoría del sistema de gestión de la seguridad que vaya a emprenderse. La auditoría del sistema de gestión de la seguridad debería garantizar que se somete a auditoría una muestra representativa de las actividades esenciales y que se entrevista al personal pertinente (incluyendo representantes de seguridad de los empleados, donde corresponda). Debería examinarse la documentación pertinente. Esto puede incluir la siguiente documentación:

- documentación del sistema de gestión de la segundad;
- declaración de la política de segundad;
- objetivos de seguridad;
- resultados de los ejercicios de practica y simulacros de seguridad;
- procedimientos;
- actas de las reuniones de seguridad;
- cualquier informe o comunicación desde la entrada en vigor de la seguridad u otras entidades reguladoras (verbal, cartas, avisos, etc.);
- registros y certificados estatutarios;
- registros de entrenamiento;
- informes previos de auditoría del sistema de gestión de la seguridad;
- demandas de acciones correctivas;
- informes de no conformidades.

Deberían hacerse posibles chequeos donde sea posible dentro de los procedimientos de auditoría del sistema de gestión de la seguridad para ayudar a evitar la errónea interpretación o aplicación de los datos, información u otros registros que se hayan reunido.

6) Resultados de la auditoría

El contenido del informe final de auditoría del sistema de gestión de la seguridad debería estar claro, preciso y completo. Debería fecharse y firmarse por el auditor. Dependiendo del caso, debería contener los siguientes elementos:

- objetivos y alcance de la auditoría del sistema de gestión de la seguridad;
- detalles del plan de auditoría del sistema de gestión de la seguridad, identificación de los miembros del equipo de auditoría y los representantes auditados, fechas de auditoría e identificación de las áreas sometidas a auditoría;
- identificación de documentos de referencia utilizados para dirigir la auditoría del sistema de gestión de la seguridad (por ejemplo, el manual de gestión de la seguridad de la norma ISO 28000);
- detalles de las no conformidades identificadas;
- la evaluación del auditor acerca del grado de conformidad con la norma ISO 28000;
- la capacidad del sistema de gestión de la seguridad para lograr los objetivos declarados de la gestión de segundad;
- la distribución del informe final de auditoría del sistema de gestión de la seguridad.

Los resultados de las auditorías del sistema de gestión de la seguridad deberían entregarse lo más pronto posible a todas las partes pertinentes, para permitir que se tomen las acciones correctivas. Se debería preparar un plan de acción de medidas remédiales convenidas junto con la identificación de las personas responsables, fechas de realización y requisitos de informe. Deberían establecerse disposiciones de supervisión de seguimiento con el fin de asegurar la implementación satisfactoria de las recomendaciones.

La dirección debería llevar a cabo una revisión de los resultados y emprender la acción correctiva eficaz (donde sea necesario hacerlo).

Deberían llevarse a cabo auditorías de seguimiento (no programadas) para revisar la implementación eficaz de las acciones correctivas.

Debería considerarse mantener confidencialidad cuando se esté recolectando y registrando la información contenida en los informes de auditoría de los sistemas de gestión de la seguridad.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- plan/programa de auditoría del sistema de gestión de la seguridad;

- procedimientos de auditoría del sistema de gestión de la seguridad;

- informes de auditoría del sistema de gestión de la seguridad, incluyendo informes de no conformidades, recomendaciones y demandas de acciones correctivas;
- informes de no conformidades sin firma/sin cierre;
- evidencia de informe a la dirección sobre los resultados de la auditoría del sistema de gestión de la seguridad.

4.6 REVISIÓN POR LA DIRECCIÓN Y MEJORA CONTINUA

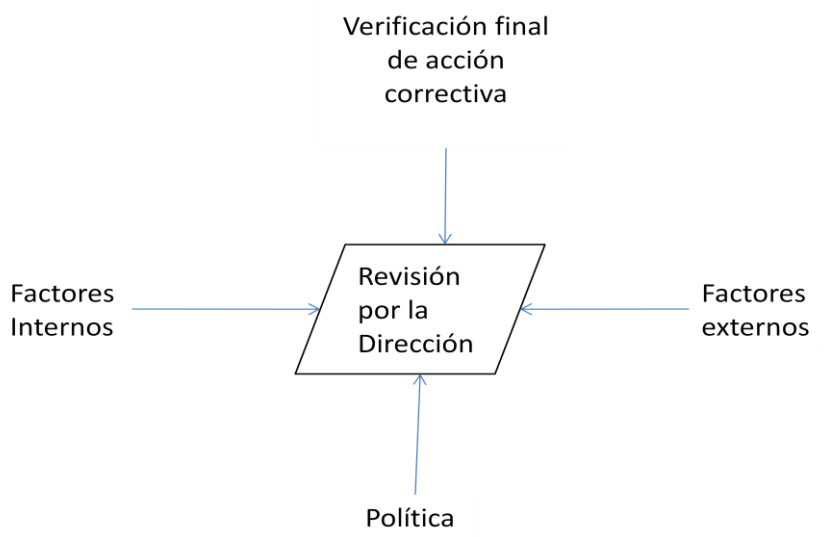

Figura 6. Revisión de la dirección

a) Requisito ISO 28000

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.

b) Propósito

La alta gerencia debería revisar la operación del sistema de gestión de la seguridad para evaluar si se está implementando totalmente y si sigue siendo conveniente y eficaz para lograr la política de seguridad y los objetivos de seguridad declarados por la organización.

La revisión también debería considerar si la política de seguridad continúa siendo apropiada. Debería establecer nuevos o actualizados objetivos de seguridad para la mejora continua, apropiados para los períodos próximo y considera si se necesitan cambios en cualquier elemento del sistema de gestión de la seguridad.

c) Entradas típicas

Las entradas típicas incluyen los siguientes elementos:

- resultados de las auditorías internas y externas del sistema de gestión de la seguridad;
- acciones correctivas efectuadas al sistema desde la revisión anterior; informes de

  ejercicios de práctica y simulacros de seguridad;
- informe del representante de la alta gerencia sobre el desempeño general del sistema;
- informes de otras personas de la organización y de las partes interesadas sobre la eficacia del sistema, en cuanto éste impacta la cadena de suministro;
- informes de identificación de amenaza a la seguridad, evaluación del riesgo y procesos de gestión del riesgo;
- efectividad de los programas de entrenamiento y conocimiento;
- el avance y la efectividad de los objetivos de la dirección de seguridad.

d) Proceso

El proceso de revisión por la dirección incluye normalmente una reunión efectuada con regularidad por la alta gerencia (por ejemplo, anualmente). La revisión debería centrarse en el desempeño global del sistema de gestión de la seguridad y no en detalles específicos, ya que éstos deberían manejarse por los medios normales dentro del sistema de gestión de la seguridad.

En la planificación de una revisión por la dirección deberían considerarse los siguientes aspectos:

- temas que van a tratarse;
- quiénes deberían asistir (gerentes, asesores especialistas en seguridad, otro personal);
- responsabilidades de los participantes individuales respeto de la revisión;
- información que va a llevarse a la revisión.

La revisión debería tratar los siguientes asuntos:

- conveniencia de la actual política de seguridad;
- establecimiento o actualización de objetivos de seguridad para la mejora continua en el período venidero;
- adecuación de los actuales procesos de identificación de amenaza a la seguridad, evaluación del riesgo y gestión del riesgo;
- actuales niveles de riesgo y la eficacia de las medidas de control existentes;
- adecuación de recursos;
- eficacia del proceso de inspección de seguridad;
- eficacia del proceso de informe del riesgo de seguridad;
- datos relacionados con la seguridad e incidentes que han ocurrido;
- casos registrados de procedimientos que no son eficaces;
- resultados de las auditorías internas y externas del sistema de gestión de la seguridad llevadas a cabo desde la revisión anterior y su eficacia;
- estado de preparación para situaciones de emergencia y disposiciones de recuperación de la seguridad;
- mejoras al sistema de gestión de la seguridad;
- resultado de cualquier investigación en cuanto a incidentes de segundad;
- una evaluación de los efectos de los cambios previsibles a la legislación, regulaciones, tecnología o inteligencia e información de seguridad.

La alta gerencia debería garantizar que el desempeño global del sistema de gestión de la segundad se informe en la reunión de revisión por la dirección. Deberían sostenerse revisiones parciales del desempeño del sistema de gestión de la seguridad a intervalos más frecuentes, si se requiere.

Las revisiones por la dirección pueden incluir una revisión de un sistema de gestión integrado, para que el resultado de la revisión de la seguridad, la calidad y otros elementos del sistema de gestión puedan considerarse en la misma reunión o durante el mismo proceso. Si se adopta este enfoque, no se debería diluir la importancia de ninguna de las partes constitutivas del sistema de gestión integrado de una organización.

e) Resultados típicos

Los resultados típicos incluyen los siguientes elementos:

- actas de cualquier reunión de revisión que se efectúe; revisiones de la política

  de seguridad y los objetivos de seguridad;
- acciones correctivas específicas por los gerentes individuales, con las fechas objetivo para su realización;
- acciones de mejora específicas, con las responsabilidades asignadas y las fechas objetivo para su realización;
- fecha para la revisión de la acción correctiva;
- áreas de énfasis que deberían reflejarse en la planificación de las futuras auditorías internas del sistema de gestión de la seguridad.

ANEXO A
(Informativo)

CORRESPONDENCIA ENTRE LAS NORMAS ISO 28000:2007, ISO 14001:2004 E ISO 9001:2000

ISO 28000:2007		ISO 14001:2004		1509001:2000	
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

(Continuación)

ISO 28000:2007		18014001:2004		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

(Final)

ISO 28000:2007		15014001:2004		1809001:2000	
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] 9001:2000, Sistemas de gestión de la calidad. Requisitos.

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

[3] ISO/IEC 17021:2006, Evaluación de la conformidad. Requisitos para los organismos que realizan auditoria y certificación de sistemas de gestión.

[4] 19011:2000, Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiente.

[5] ISO 28001:2007, Specification for Security Management Systems for the Supply Chain.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Security Management Systems forthe Supply Chain. Guidelines forthe Implementation of\SO* 28000, ISO: 28004: 2007(E), p 56.

ICONTEC

NTC-ISO 28000 Sistemas de gestión de la seguridad para la cadena de suministro;

NTC-ISO 28001, Sistemas de gestión de la seguridad para la cadena de suministro. Mejores prácticas para implementar evaluaciones y planes para la seguridad de la cadena de suministro. Requisitos y orientación

NTC-ISO 28004, Sistemas de gestión de la seguridad para la cadena de suministro. Directrices para la implementación de la norma ISO 28000.

ISBN: 978-958-9383-85-8

9 789589 383858