NORMA INTERNACIONAL

ISO 28000:2007

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

Introducción

Esta norma internacional ha sido desarrollada como respuesta a la exigencia de la industria para una norma de gestión de la seguridad. Su objetivo principal es mejorar la seguridad en las cadenas de suministro. Esta es una norma de Alta Dirección que le permite 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 reglamentarios que la Organización cumple. Si se determinan 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 con 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.

Esta norma internacional está intencionada para aplicar en casos donde las cadenas de suministro de una organización, tengan que ser manejadas de forma segura. Un acercamiento formal a gestión de la seguridad puede contribuir directamente con la capacidad del negocio y credibilidad de la organización.

El cumplimiento con esta norma internacional no lleva en sí mismo inmunidad de las obligaciones legales. Para las organizaciones que así lo quieran, el cumplimiento con el sistema de gestión de la seguridad con esta norma internacional puede ser verificado por un proceso de auditoría externa ó interna.

Esta norma internacional está basada en el formato ISO adoptado por ISO 14001:2004 debido a su enfoque de sistema de gestión basado en el riesgo. Sin embargo, organizaciones que han adoptado un proceso de acercamiento a los sistemas de gestión (ej. ISO 9001:2000) podrán utilizar su sistema de gestión actual como la base para un sistema de gestión de la seguridad como se prescribe en esta norma internacional. No es la intención de esta norma internacional, el duplicar los requisitos gubernamentales y normas con respecto a la gestión de la seguridad de la cadena de suministro, por la cual la organización ya ha sido certificada ó se ha verificado cumplimiento. La verificación se puede llevar a cabo por una organización aceptable por primera, segunda o tercera parte.

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

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

1 Alcance

Esta norma internacional especifica los requisitos para un sistema de gestión de la seguridad, incluyendo aquellos aspectos críticos para garantizar 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 ó influenciadas por organizaciones que impactan en la seguridad de la cadena de suministro. Estos otros aspectos deberían ser considerados directamente, dónde y cuándo éstos tengan un impacto en la gestión de seguridad, incluyendo el transporte de estos bienes a lo largo de la cadena de suministro.

Esta norma internacional es aplicable a todos los tamaños de organizaciones, de pequeñas a multinacionales, en manufactura, servicios, almacenamiento ó transporte en cualquier etapa de la cadena de producción ó de suministro que tenga la intención de:

a) Establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad.
b) Asegurar conformidad con la política de gestión de la seguridad establecida.
c) Demostrar dicha conformidad a otros.
d) Buscar certificación/registro de su sistema de gestión de seguridad por parte de un organismo de de certificación de tercera parte acreditado; o
e) Hacer una auto-determinación y auto-declaración de conformidad con esta norma internacional.

No es la intención de esta norma internacional exigir demostración duplicada de conformidad.

Las organizaciones que elijan certificación de un tercero, pueden demostrar además que están contribuyendo significativamente con la seguridad de la cadena de suministro.

2 Referencias Normativas

No hay referencias normativas citadas. Esta cláusula está incluida para retener una numeración de cláusulas similar al de otras normas de sistemas de gestión.

3 Términos y Definiciones

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

3.1 Instalación

Planta, maquinaria, propiedad, edificios, vehículos, embarcaciones, instalaciones portuarias y otros elementos de infraestructura ó plantas y sistemas relacionados, que tienen 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 misma.

3.2 Seguridad

Resistencia a actos intencionales, sin autorización, diseñados para causar perjuicio o daño a, ó 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 de manera óptima sus riesgos y las amenazas e impactos potenciales asociados derivados de ellos.

3.4 Objetivo de Gestión de la seguridad
Resultado ó logro específico de seguridad requerido para cumplir con la política de gestión de seguridad.

3.5 Política de Gestión de la seguridad
Intenciones y direcciones generales de una organización, relacionadas con la seguridad y estructura para el control de procesos y actividades relacionados con 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
Son los medios mediante 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 lograr un objetivo de la gestión de la seguridad.

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

NOTA Ejemplos incluyen clientes, accionistas, entidades financieras, aseguradores, reguladores, cuerpos reglamentarios, empleados, contratantes, proveedores, organizaciones laborales ó 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 ó servicios al usuario final, incluidos los medios de transporte.

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

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

3.9.2 Aguas arriba
Se refiere a las acciones, procesos y movimientos de la carga dentro de la cadena de suministro que ocurren antes de que la carga se encuentre bajo el control directo operacional de la organización, incluyendo pero no limitado al seguro, finanzas, gestión de información y el empaque, almacenamiento y transferencia de la carga.

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

NOTA: La Alta Dirección, especialmente en una organización multinacional grande, puede no estar personalmente involucrado como se menciona en esta norma internacional: 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, para lograr mejoramientos en el desempeño general de la seguridad, de manera coherente con la política de seguridad de la organización.

Otras definiciones importantes:

Amenaza: Cualquier posible acción o serie de acciones intencionales con daño potencial a cualquiera de las 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

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

4. 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 de la seguridad, valorar los riesgos y controlar y mitigar sus consecuencias.

La organización debe mejorar continuamente su eficacia de acuerdo con los requisitos establecidos en toda la cláusula 4.

La organización debe definir el alcance de su sistema de gestión de la seguridad. Cuando una organización opte por contratar externamente cualquier proceso que afecte la conformidad con estos requisitos, la organización debe asegurar que dichos procesos sean controlados. 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 aplicable actual, los requisitos reglamentarios y estatutarios y con 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, incluyendo 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 sea 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 escoger entre tener una política detallada de gestión de seguridad para uso interno que podría proporcionar suficiente información y dirección para manejar el sistema de gestión de seguridad (partes que pueden ser confidenciales) ó de tener una versión resumida (no – confidencial) que contenga los objetivos generales para la diseminación para sus partes interesadas y otras partes involucradas.

4.3 Valoración del Riesgo de Seguridad y Planeación

4.3.1 Valoración del riesgo de seguridad

La organización debe establecer y mantener procedimientos para la identificación y valoración 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, valoración y métodos de control de amenazas y riesgos de la seguridad deberían, como mínimo, ser apropiados a la naturaleza y escala de las operaciones. Esta valoración debe considerar la probabilidad de un evento y de todas sus consecuencias, que deben incluir:

a) Amenazas y riesgos de fallas físicas, como falla funcional, daño incidental, daño malicioso, terrorista ó acción criminal;
b) Amenazas y riesgos operacionales, incluyendo el control de la seguridad, los factores humanos y otras actividades que afectan el desempeño, la condición o la seguridad de la organización.
c) Eventos ambientales naturales (tormenta, inundación, etc.), que pueden hacer que las medidas y equipos de seguridad resulten ineficaces.
d) Factores ajenos al control de la organización, tales como fallas en equipos y servicios suministrados externamente;
e) Amenazas y riesgos de las partes interesadas, tales como fallas para cumplir con los requisitos reglamentarios o daño a la reputación ó marca;
f) Diseño e instalación del equipo de seguridad, incluyendo 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 valoraciones y los efectos de estos controles y, cuando sea apropiado, debe proporcionar elementos de entrada a:

a) Los Objetivos y metas de la 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, incluyendo los niveles de contratación de personal;
e) La Identificación de necesidades de formación y habilidades (ver 4.4.2);
f) El Desarrollo de controles operacionales (ver 4.4.6);
g) La estructura general de gestión de amenazas y de riesgos de la organización;

La organización debe documentar y mantener actualizada la anterior información.

La metodología de la organización para la identificación de la amenaza y valoración del riesgo debe:

a) Estar definida con respecto a su alcance, naturaleza y programación en el tiempo para asegurar que sea proactiva en lugar de ser reactiva;

b) Incluir la recolección de información relacionada con amenazas y riesgos de la seguridad;
c) Proporcionar la clasificación de amenazas y riesgos y la identificación de los que deben evitarse, eliminarse ó controlarse;
d) Proporcionar el seguimiento de las acciones para asegurar su eficacia y oportuna implementación (ver 4.5.1).

4.3.2 Requisitos legales y reglamentarios de seguridad

La organización debe establecer, implementar y mantener un procedimiento:

a) para identificar y tener acceso a los requisitos legales aplicables y otros requisitos a los que se suscribe la organización relacionados con las 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 esta información actualizada y debe comunicar la información pertinente sobre requisitos legales y otros requisitos a sus empleados y otras terceras partes pertinentes, incluyendo 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 y ser coherentes con la política. Al establecer y revisar sus objetivos, la 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, incluyendo los contratistas, con la intención que estas personas sean conscientes de sus obligaciones individuales;
d) Revisarse periódicamente para asegurar que sigan siendo pertinentes y coherentes con la política de gestión de la seguridad. Cuando sea necesario, los objetivos de gestión de la seguridad deben ser corregidos.

4.3.4 Metas de Gestión de la Seguridad

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

Estas metas deben:

a) tener un nivel de detalle apropiado;
b) ser específicas, medibles, alcanzables, pertinentes y basadas en el tiempo (cuando sea aplicable);
c) Comunicarse a todos los empleados y terceros pertinentes, incluyendo contratistas, con la intención de que estas personas estén conscientes de sus obligaciones individuales;
d) Revisarse periódicamente para asegurar que se mantengan pertinentes y coherentes con la política y objetivos de gestión de la seguridad. Donde sea necesario, las metas de gestión de seguridad deben ser ajustadas consecuentemente.

4.3.5 Programas de Gestión de la Seguridad

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

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

Esto debe incluir documentación que describa:

a) La responsabilidad y autoridad designada para lograr los objetivos y metas de la gestión de la seguridad;
b) Los medios y la escala en el tiempo mediante los cuales las metas y objetivos serán logrados.

Los programas de gestión de la seguridad deben revisarse periódicamente para asegurar que se mantienen efectivos y coherentes con los objetivos y metas. Los programas deben ser ajustados cuando sea necesario.

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 autoridades, coherente con el logro de su política de gestión de seguridad, objetivos, metas y programas.

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

La Alta Dirección debe proporcionar evidencia de su compromiso con el desarrollo e implementación de los procesos del sistema de gestión de la seguridad 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 por el 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 asegurar que los objetivos y metas sean implementados.
c) Identificar y hacer seguimiento a los requisitos y expectativas de las partes interesadas de la organización y tomar acciones apropiadas y oportunas para manejar estas expectativas;
d) Asegurar la disponibilidad de recursos adecuados.
e) Considerar el impacto adverso que la política, objetivos, metas, programas de gestión de seguridad, etc. puedan tener sobre otros aspectos de la organización;
f) Asegurar que otros programas de seguridad generados por otras partes de la organización complementen el sistema de gestión de la seguridad;
g) Comunicar a la organización la importancia de cumplir con los requisitos de gestión de la seguridad para cumplir con su política;
h) Asegurar que las amenazas y riesgos relacionados con la seguridad sean evaluados y se incluyan en las valoraciones de amenazas y riesgos de la organización de forma apropiada;
i) Asegurar la viabilidad de los objetivos, metas y programas de gestión de la seguridad.

4.4.2 Competencia, Formación y Toma de Conciencia

La organización debe asegurar que el personal responsable por el diseño, operación y gestión de los equipos de seguridad y procesos esté calificado de manera adecuada en términos de educación, formación y/o experiencia. 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, incluyendo los requisitos de preparación y de respuesta ante emergencias;
c) Las consecuencias potenciales que tiene para la seguridad de la organización desviarse de los procedimientos de operación especificados.

Se deben mantener registros de competencia y formación.

4.4.3 Comunicación

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

Debido a la naturaleza confidencial de cierta 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, pero sin limitarse, a lo siguiente:

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 a documentos relacionados,
d) los documentos, incluyendo registros, requeridos por esta norma internacional, y
e) los documentos, incluyendo registros, determinados por la organización como necesarios para asegurar la planeación operación y control eficaces de los procesos que se relacionan a sus amenazas y riesgos de 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 requerida por la cláusula 4 de esta norma internacional para asegurar 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) estén disponibles versiones actuales de documentos, datos e información pertinentes en todas las locaciones donde se realicen operaciones esenciales para el funcionamiento efectivo del sistema de gestión de la seguridad;
d) los documentos, datos e información obsoletos retenidos por propósitos de preservación legal ó de conocimiento son identificados, además que se asegure 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 de conocimiento;
f) estos documentos, datos e información sean seguros y si son archivados de forma electrónica, deben tener copia de seguridad y se pueden ser recuperados.

4.4.6 Control Operacional

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

a) su política de gestión de la seguridad;

b) el control de las actividades y la mitigación de amenazas identificadas como de alto riesgo (riesgo significativo);
c) el cumplimiento con requisitos legales, estatutarios y otros requisitos de reglamentación de 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 asegurar de que estas operaciones y actividades se lleven a cabo bajo condiciones especificadas al:

a) establecer, implementar y mantener procedimientos documentados para controlar situaciones donde su ausencia podría llevar a no lograr las operaciones y actividades listadas en 4.4.6 a) a f);
b) evaluar cualquier amenaza que surja de las actividades Aguas arriba de la cadena de suministro y aplicar controles para mitigar estos impactos en la organización y otros operadores de la cadena de suministro Aguas abajo;
c) establecer y mantener los requisitos para bienes y servicios que tengan impacto sobre la seguridad y comunicarlas a proveedores y contratistas;

Estos procedimientos 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 organizacional, funciones ó responsabilidades revisadas y actualizadas;
b) la política, metas, objetivos y programas de gestión de seguridad revisados y actualizados;
c) los procedimientos y procesos revisados y actualizados;
d) la introducción de nueva infraestructura, equipos ó tecnología de seguridad, que puedan incluir hardware y/ó software;
e) la introducción de nuevos contratistas, proveedores ó 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 prevenir y mitigar las consecuencias probables que puedan estar asociadas con las mismas.

Los planes y procedimientos deben incluir información acerca de la disposición y mantenimiento de cualquier equipo, servicios e instalaciones identificados que puedan necesitarse durante ó después de situaciones de emergencia ó incidentes.

La organización debe revisar periódicamente la eficacia de sus planes y procedimientos de preparación y respuesta ante emergencias y recuperación de la seguridad, particularmente después de la ocurrencia de incidentes ó situaciones de emergencia causadas 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 monitoreo 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. La organización debe considerar las amenazas y riesgos asociadas con la seguridad, incluyendo mecanismos de deterioro potencial y sus consecuencias, cuando se establece la frecuencia para hacer el seguimiento y medición de los parámetros de desempeño claves.

Estos procedimientos deben proporcionar:

a) tanto medidas cuantitativas como cualitativas, apropiadas para las necesidades de la organización;
b) seguimiento del grado en que se cumplen los objetivos, metas y políticas de gestión de la seguridad;
c) medidas proactivas de desempeño que monitorean la conformidad con los programas de gestión de la seguridad, los criterios de control operacionales y la legislación aplicable, los requisitos estatutarios otros requisitos de reglamentación sobre seguridad;
d) medidas reactivas de desempeño para hacer el seguimiento de deterioros, pérdidas, fallas, incidentes, no conformidades relacionados con seguridad (incluyendo casi – fallas y falsas alarmas) 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, 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, y sus resultados serán retenidos por el tiempo suficiente para cumplir con la legislación y 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, reportes después de incidentes, lecciones aprendidas, evaluaciones de desempeño y ejercicios. Los cambios significativos en estos factores deben ser reflejados inmediatamente en el procedimiento(s).

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

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

4.5.3 Fallas relacionadas con 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 fallas potenciales de seguridad y poder evitar que ocurran;
b) la investigación de los siguientes aspectos relacionados con seguridad:
    1) fallas incluyendo casi fallas y falsa alarma;
    2) incidentes y situaciones de emergencia;
    3) no conformidades;
c) tomar acción para mitigar todas las consecuencias de dichas fallas, incidentes ó no conformidades;
d) el inicio y fin de acciones correctivas;
e) la confirmación de la eficacia de las acciones correctivas tomadas.

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

Cualquier acción correctiva ó preventiva tomada para eliminar las causas de no conformidades actuales y potenciales debe ser apropiada para la magnitud de los problemas y proporcional con las posibles amenazas y riesgos del gestión de seguridad. La organización debe implementar y registrar todos los cambios en los procedimientos documentados que sean el resultado de una acción correctiva y preventiva e incluirá el entrenamiento requerido donde sea necesario.

4.5.4 Control de Registros

La organización debe establecer y mantener los registros necesarios para demostrar conformidad con los requisitos de su sistema de gestión de la seguridad y de esta norma, y de sus logros.

La organización debe establecer, implementar y mantener procedimientos para la identificación, almacenamiento, protección, retención, recuperación y disposición de registros.

Los registros deben ser legibles, identificables y trazables.

La documentación electrónica y digital debe tener copia de seguridad y con acceso sólo de personal autorizado.

4.5.5 Auditoria

La organización debe establecer, implementar y mantener un programa de auditoría de gestión de la seguridad y debe asegurar que las auditorias del sistema de gestión de la seguridad se lleven a cabo en intervalos planeados, para:

a) determinar si el sistema de gestión de la seguridad:
   1) cumple con las disposiciones planificadas para la gestión de la seguridad, incluyendo los requisitos de toda la cláusula 4 de esta norma;
   2) ha sido implementado y mantenido adecuadamente;
   3) es eficaz para cumplir la política y objetivos de gestión de la seguridad de la organización;
b) revisar los resultados de auditorías previas y las acciones tomadas para rectificar no conformidades;
c) proporcionar información a la Dirección sobre resultados de auditorias
d) verificar el despliegue apropiado de los equipos y el personal de seguridad

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

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 planeados, para asegurar su adecuación, conveniencia y eficacia continuas. Las revisiones deben incluir oportunidades de mejora y la necesidad de cambios en el sistema de gestión de la seguridad, incluyendo política de seguridad y objetivos, amenazas y riesgos de seguridad. Se deben mantener registros de las revisiones por la dirección.

La Información de entrada de las revisiones por la dirección, deben incluir:

a) resultados de las auditorias y evaluaciones de conformidad con requisitos legales y con otros requisitos a los que se suscribe la organización;
b) comunicaciones de partes interesadas, incluyendo quejas;
c) el desempeño de seguridad de la organización;
d) el grado de cumplimiento de los objetivos y metas,
e) estado de acciones correctivas y preventivas,
f) acciones de seguimiento de revisiones por la dirección anteriores,
g) circunstancias cambiantes, incluyendo desarrollos en requisitos legales y otros relacionados con sus aspectos de seguridad y
h) recomendaciones de mejora.

Las conclusiones de las revisiones de gestión deben incluir todas las decisiones y acciones relacionadas con posibles cambios de la política de seguridad, objetivos, metas y otros elementos del sistema de gestión de la seguridad, coherente con el compromiso con la mejora continua.